

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 9 - 1 6 2 8 5 9

(43) 公開日 平成 9 年 (1997) 6 月 20 日

| (51) Int. Cl. | 識別記号 | 庁内整理番号 | F I       | 技術表示箇所 |
|---------------|------|--------|-----------|--------|
| H04L 9/20     |      |        | H04L 9/00 | 653    |
| 9/16          |      |        |           | 643    |
| H04N 7/24     |      |        | H04N 7/13 | 7      |
| 7/167         |      |        | 7/167     | 7      |

審査請求 未請求 請求項の数 23 O L (全 27 頁)

(21) 出願番号 特願平 7 - 3 1 9 4 2 1

(22) 出願日 平成 7 年 (1995) 12 月 7 日

(71) 出願人 0 0 0 0 0 5 2 2 3

富士通株式会社

神奈川県川崎市中原区上小田中 4 丁目 1 番  
1 号

(72) 発明者 小川 清隆

神奈川県川崎市中原区上小田中 1 0 1 5 番  
地 富士通株式会社内

(72) 発明者 小桧山 清之

神奈川県川崎市中原区上小田中 1 0 1 5 番  
地 富士通株式会社内

(74) 代理人 弁理士 平戸 哲夫

最終頁に続く

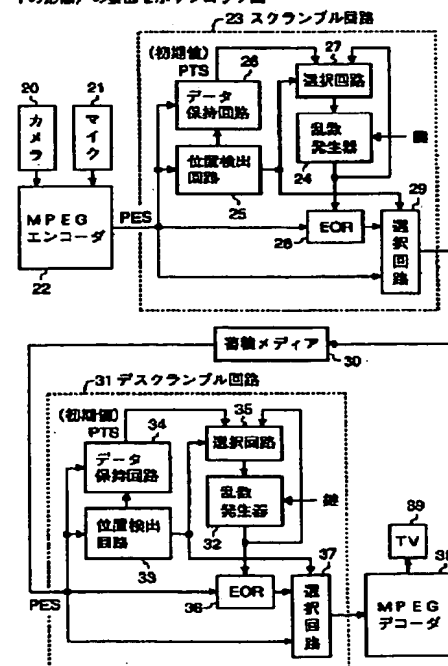
(54) 【発明の名称】 スクランブル方法及び装置、デスクランブル方法及び装置、並びに、データ伝達方法及びシステム

(57) 【要約】

【課題】 MPEG 標準のストリームの伝達系などに適用して好適なデータ伝達システムに関し、機密性の高いデータ伝達を実現する。

【解決手段】 スクランブル回路 23 の乱数発生器 24 には、スクランブルの対象とされているパケット・データ部のストリームごとに、値を一定としない PTS (再生出力の時刻管理情報) を初期値として供給し、デスクランブル回路 31 の乱数発生器 32 には、スクランブルされているパケット・データ部のストリームごとに、PTS を初期値として供給する。

本発明のデータ伝達方法の実施の第 1 の形態の実施に使用するデータ伝達システム (本発明のデータ伝達システムの実施の第 1 の形態) の要部を示すブロック図



1

## 【特許請求の範囲】

【請求項 1】第 1 のストリーム部の後方に第 2 のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームのうち、スクランブルの対象とされている第 2 のストリーム部を乱数発生器を使用してスクランブルするスクランブル方法であって、前記スクランブルの対象とされている第 2 のストリーム部ごとに、前記第 1 のストリーム部内のデータ値が一定でない所定のデータのデータ値を初期値として前記乱数発生器に供給することにより、前記スクランブルの対象とされている第 2 のストリーム部をスクランブルすることを特徴とするスクランブル方法。

【請求項 2】前記スクランブルの対象とされている第 2 のストリーム部と同一の単位ストリームの第 1 のストリーム部内に前記所定のデータが存在しない場合には、前記所定のデータが存在する第 1 のストリーム部のうち、前記所定のデータが存在しない第 1 のストリーム部の直前の第 1 のストリーム部内の前記所定のデータのデータ値を初期値として前記乱数発生器に供給することにより、前記スクランブルの対象とされている第 2 のストリーム部をスクランブルすることを特徴とする請求項 1 記載のスクランブル方法。

【請求項 3】前記第 1 のストリーム部の後方に第 2 のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームは、MPEG 標準のストリームであり、前記第 1 のストリーム部は、パケット・ヘッダ部のストリーム、前記第 2 のストリーム部は、パケット・データ部又はペイロード部のストリーム、前記所定のデータは、プレゼンテーション・タイム・スタンプ又はデコーディング・タイム・スタンプ又は巡回カウンタ又はデコーディング・タイム・スタンプと巡回カウンタとを組み合わせ又は演算したデータであることを特徴とする請求項 1 又は 2 記載のスクランブル方法。

【請求項 4】前記第 1 のストリーム部の後方に第 2 のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームの全部又は一部を複数列のストリームにパラレル変換してスクランブルすることを特徴とする請求項 1、2 又は 3 記載のスクランブル方法。

【請求項 5】第 1 のストリーム部の後方に第 2 のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームのうち、スクランブルの対象とされている第 2 のストリーム部をスクランブルするスクランブル装置であって、乱数を発生する乱数発生器と、前記スクランブルの対象とされている第 2 のストリーム部ごとに、前記第 1 のストリーム部内のデータ値が一定でない所定のデータのデータ値を初期値として前記乱数発生器に供給する初期値供給回路と、前記スクランブルの対象とされている第 2 のストリーム部と前記乱数発生器から出力される乱数とを論理演算して前記スクランブルの対象とされている第 2 のストリーム部をスクランブルす

2

る論理演算回路とを備えていることを特徴とするスクランブル装置。

【請求項 6】前記初期値供給回路は、前記スクランブルの対象とされている第 2 のストリーム部と同一の単位ストリームの第 1 のストリーム部内に前記所定のデータが存在しない場合には、前記所定のデータが存在する第 1 のストリーム部のうち、前記所定のデータが存在しない第 1 のストリーム部の直前の第 1 のストリーム部内の前記所定のデータのデータ値を初期値として前記乱数発生器に供給することを特徴とする請求項 5 記載のスクランブル装置。

【請求項 7】前記第 1 のストリーム部の後方に第 2 のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームは、MPEG 標準のストリームであり、前記第 1 のストリーム部は、パケット・ヘッダ部のストリーム、前記第 2 のストリーム部は、パケット・データ部又はペイロード部のストリーム、前記所定のデータは、プレゼンテーション・タイム・スタンプ又はデコーディング・タイム・スタンプ又は巡回カウンタ又はデコーディング・タイム・スタンプと巡回カウンタとを組み合わせ又は演算したデータであることを特徴とする請求項 5 又は 6 記載のスクランブル装置。

【請求項 8】前記初期値供給回路は、前記所定のデータの位置及び前記第 2 のストリーム部の開始位置を検出する位置検出回路と、この位置検出回路が前記所定のデータの位置を検出した場合、前記所定のデータのデータ値を保持するデータ保持回路とを備えていることを特徴とする請求項 5、6 又は 7 記載のスクランブル装置。

【請求項 9】前記第 1 のストリーム部の後方に第 2 のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームを複数列のストリームにパラレル変換するシリアル／パラレル変換回路を有し、前記データ保持回路及び前記論理演算回路は、複数列のストリームに対応することができるよう構成されていると共に、前記論理演算回路から出力される複数列のストリームをシリアル変換するパラレル／シリアル変換回路を備えていることを特徴とする請求項 5、6、7 又は 8 記載のスクランブル装置。

【請求項 10】前記位置検出回路による処理を CPU によるソフトウェア処理により行い、規格の異なる複数のストリームに対応することができるよう構成されていることを特徴とする請求項 8 又は 9 記載のスクランブル装置。

【請求項 11】第 1 のストリーム部の後方に第 2 のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームのうち、デスクランブルの対象とされている第 2 のストリーム部を乱数発生器を使用してデスクランブルするデスクランブル方法であって、前記デスクランブルの対象とされている第 2 のストリーム部ごとに、前記第 1 のストリーム部内のデータ値が一定で

50

ない所定のデータのデータ値を初期値として前記乱数発生器に供給することにより、前記デスクランブルの対象とされている第 2 のストリーム部をデスクランブルすることを特徴とするデスクランブル方法。

【請求項 1 2】前記デスクランブルの対象とされている第 2 のストリーム部と同一の単位ストリームの第 1 のストリーム部内に前記所定のデータが存在しない場合には、前記所定のデータが存在する第 1 のストリーム部のうち、前記所定のデータが存在しない第 1 のストリーム部の直前の第 1 のストリーム部内の前記所定のデータのデータ値を初期値として前記乱数発生器に供給することにより、前記デスクランブルの対象とされている第 2 のストリーム部をデスクランブルすることを特徴とする請求項 1 1 記載のデスクランブル方法。

【請求項 1 3】前記第 1 のストリーム部の後方に第 2 のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームは、MPEG 標準のストリームであり、前記第 1 のストリーム部は、パケット・ヘッダ部のストリーム、前記第 2 のストリームは、パケット・データ部又はペイロード部のストリーム、前記所定のデータは、プレゼンテーション・タイム・スタンプ又はデコーディング・タイム・スタンプ又は巡回カウンタ又はデコーディング・タイム・スタンプと巡回カウンタとを組み合わせ又は演算したデータであることを特徴とする請求項 1 1 又は 1 2 記載のデスクランブル方法。

【請求項 1 4】前記第 1 のストリーム部の後方に第 2 のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームの全部又は一部を複数のストリームにパラレル変換してデスクランブルすることを特徴とする請求項 1 1、1 2 又は 1 3 記載のデスクランブル方法。

【請求項 1 5】第 1 のストリーム部の後方に第 2 のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームのうち、デスクランブルの対象とされている第 2 のストリーム部をデスクランブルするデスクランブル装置であって、乱数を発生する乱数発生器と、前記デスクランブルの対象とされている第 2 のストリーム部ごとに、前記第 1 のストリーム部内のデータ値が一定でない所定のデータのデータ値を初期値として前記乱数発生器に供給する初期値供給回路と、前記デスクランブルの対象とされている第 2 のストリーム部と前記乱数発生器から出力される乱数とを論理演算して前記デスクランブルの対象とされている第 2 のストリーム部をデスクランブルする論理演算回路とを備えていることを特徴とするデスクランブル装置。

【請求項 1 6】前記初期値供給回路は、前記デスクランブルの対象とされている第 2 のストリーム部と同一の単位ストリームの第 1 のストリーム部内に前記所定のデータが存在しない場合には、前記所定のデータが存在する第 1 のストリーム部のうち、前記所定のデータが存在し

ない第 1 のストリーム部の直前の第 1 のストリーム部内の前記所定のデータのデータ値を初期値として前記乱数発生器に供給することを特徴とする請求項 1 5 記載のデスクランブル装置。

【請求項 1 7】前記第 1 のストリーム部の後方に第 2 のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームは、MPEG 標準のストリームであり、前記第 1 のストリーム部は、パケット・ヘッダ部のストリーム、前記第 2 のストリームは、パケット・データ部又はペイロード部のストリーム、前記所定のデータは、プレゼンテーション・タイム・スタンプ又はデコーディング・タイム・スタンプ又は巡回カウンタ又はデコーディング・タイム・スタンプと巡回カウンタとを組み合わせ又は演算したデータであることを特徴とする請求項 1 5 又は 1 6 記載のデスクランブル装置。

【請求項 1 8】前記初期値供給回路は、前記所定のデータの位置及び前記第 2 のストリーム部の開始位置を検出する位置検出回路と、この位置検出回路が前記所定のデータの位置を検出した場合、前記所定のデータのデータ値を保持するデータ保持回路とを備えていることを特徴とする請求項 1 5、1 6 又は 1 7 記載のデスクランブル装置。

【請求項 1 9】前記第 1 のストリーム部の後方に第 2 のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームを複数列のストリームにパラレル変換するシリアル／パラレル変換回路を有し、前記データ保持回路及び前記論理演算回路は、複数列のストリームに対応することができるように構成されていると共に、前記論理演算回路から出力される複数列のストリームをシリアル変換するパラレル／シリアル変換回路を備えていることを特徴とする請求項 1 5、1 6、1 7 又は 1 8 記載のデスクランブル装置。

【請求項 2 0】前記位置検出回路による処理を CPU によるソフトウェア処理により行い、規格の異なる複数のストリームに対応することができるように構成されていることを特徴とする請求項 1 8 又は 1 9 記載のデスクランブル装置。

【請求項 2 1】カード化されると共に、身分証明データを記憶する記憶回路を有し、外部装置から前記身分証明データを認証した場合のみ、前記外部装置から前記乱数発生器にアクセスできるように構成されていることを特徴とする請求項 1 5、1 6 又は 1 7 記載のデスクランブル装置。

【請求項 2 2】伝達元において、第 1 のストリーム部の後方に第 2 のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームについて、請求項 1、2、3 又は 4 記載のスクランブル方法を実行し、これにより得られるストリームを伝達メディアを介して伝達先に伝達し、前記伝達先において請求項 1 1、1 2、1 3 又は 1 4 記載のデスクランブル方法を実行し、

10

20

30

40

50

前記第 1 のストリーム部の後方に第 2 のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームを復元する工程を含んでいることを特徴とするデータ伝達方法。

【請求項 23】請求項 5、6、7、8、9 又は 10 記載のスクランブル装置を有し、第 1 のストリーム部の後方に第 2 のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームをスクランブルの対象とされている第 2 のストリーム部をスクランブルしてなるストリームに変換して伝達メディアに伝達する伝達元と、請求項 15、16、17、18、19、20 又は 21 記載のデスクランブル装置を有し、前記伝達メディアから供給されるストリームを前記第 1 のストリーム部の後方に第 2 のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームに復元する伝達先とを備えていることを特徴とするデータ伝達システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタル動画像符号化（圧縮）、音響符号化及びその多重・分離方法についての国際標準である MPEG（Moving Picture Experts Group）標準のストリーム（ビット列）の伝達系などに適用して好適なスクランブル方法及び装置、デスクランブル方法及び装置、並びに、データ伝達方法及びシステムに関する。

【0002】

【従来の技術】従来、データ伝達システムとして、例えば、図 12 に、その要部を示すようなものが知られている。

【0003】図 12 中、1 は映像データを得るためのカメラ、2 は音声データを得るためのマイク、3 はカメラ 1 により得られる映像データとマイク 2 により得られる音声データとを符号化して時分割多重し、付加データを配列したパケット・ヘッダ部と、映像データや音声データを配列したパケット・データ部とからなる MPEG 標準のストリームにエンコードする MPEG エンコーダである。

【0004】また、4 は MPEG エンコーダ 3 から出力されるストリームをパケット・データ部のストリームがスクランブルされてなるストリームに変換するスクランブル回路である。

【0005】このスクランブル回路 4 において、5 は鍵信号により指定される系列の乱数を発生する乱数発生器、6 は MPEG エンコーダ 3 から出力されるストリームのうちのパケット・データ部のストリームと乱数発生器 5 から出力される乱数とを排他的論理和（以下、EOR という）処理する EOR 回路である。

【0006】また、7 は MPEG エンコーダ 3 から出力されるストリームのうちのパケット・ヘッダ部のスト

ームと、EOR 回路 6 から出力されるストリームとを選択して出力する選択回路である。

【0007】また、8 はディスク、テープ等の蓄積メディアや、衛星放送、CATV 等の放送メディア等、スクランブル回路 4 から出力されるストリームの伝達媒体である伝達メディアである。

【0008】また、9 は伝達メディア 8 を介して伝達されるスクランブル回路 4 から出力されたストリームをパケット・データ部のストリームがデスクランブルされてなるストリームに変換するデスクランブル回路である。

【0009】このデスクランブル回路 9 において、10 は乱数発生器 5 と同一の回路構成の乱数発生器であり、この乱数発生器 10 には乱数発生器 5 に使用された鍵信号と同一内容の鍵信号が供給される。

【0010】また、11 は伝達メディア 8 を介して伝達されるスクランブル回路 4 から出力されたストリームのうちのパケット・データ部のストリームと、乱数発生器 10 から出力される乱数とを EOR 処理する EOR 回路である。

【0011】また、12 は伝達メディア 8 を介して伝達されるスクランブル回路 4 から出力されたストリームのうちのパケット・ヘッダ部のストリームと、EOR 回路 11 から出力されるストリームとを選択して出力する選択回路である。

【0012】また、13 はデスクランブル回路 9 から出力されるストリームから映像データと音声データとを分離し、更に、これらを復号化する MPEG デコーダ、14 は MPEG デコーダ 13 から出力される映像データ及び音声データが供給されるテレビジョン受像機（TV）である。

【0013】このデータ伝達システムは、MPEG エンコーダ 3 から出力される MPEG 標準のストリームをパケット・データ部のストリームをスクランブルしてなるストリームとして伝達することによって、不法なコピーからパケット・データを保護しようとするものである。

【0014】

【発明が解決しようとする課題】しかし、このデータ伝達システムにおいては、例えば、図 13 に示すように、MPEG エンコーダ 3 からパケット・データ部のストリームとして a1、a2、a3・・・が出力されると共に、乱数発生器 5、10 から乱数 c1、c2、c3・・・が出力される場合、EOR 回路 6 の出力は、

【0015】

【数 1】

$$a1 \oplus c1, a2 \oplus c2, a3 \oplus c3 \dots$$

【0016】となり、これが選択回路 7 から出力され、EOR 回路 11 に入力されることになるので、EOR 回路 11 から出力されるストリームは、a1、a2、a3・・・となる。したがって、EOR 回路 11 に入力されるストリーム

【 0 0 1 7 】

【 数 2 】

 $a1 \oplus c1, a2 \oplus c2, a3 \oplus c3 \dots$ 

【 0 0 1 8 】 と、E O R 回路 1 1 から出力されるストリーム  $a 1$ 、 $a 2$ 、 $a 3 \dots$  とを E O R 回路 1 5 で E O R 処理すると、乱数発生器 1 0 から出力される乱数  $c 1$ 、 $c 2$ 、 $c 3 \dots$  を得ることができる。

【 0 0 1 9 】 このように、このデータ伝達システムにおいては、鍵信号が不明でも、乱数発生器 1 0 から出力される乱数パターンが容易にコピーされてしまい、スクランブルされたバケット・データについてもデスクランブルされてしまうおそれがあるという問題点があった。

【 0 0 2 0 】 本発明は、かかる点に鑑み、機密性の高いデータ伝達を実現することができるようにしたスクランブル方法及び装置、デスクランブル方法及び装置、並びに、データ伝達方法及びシステムを提供することを目的とする。

【 0 0 2 1 】

【課題を解決するための手段】 本発明のスクランブル方法は、第 1 のストリーム部の後方に第 2 のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームのうち、スクランブルの対象とされている第 2 のストリーム部を乱数発生器を使用してスクランブルするスクランブル方法であって、前記スクランブルの対象とされている第 2 のストリーム部ごとに、前記第 1 のストリーム部内のデータ値が一定でない所定のデータのデータ値を初期値として前記乱数発生器に供給することにより、前記スクランブルの対象とされている第 2 のストリーム部をスクランブルするするというものである。

【 0 0 2 2 】 本発明のスクランブル方法を使用する場合には、デスクランブルは、スクランブルされている第 2 のストリーム部ごとに、第 1 のストリーム部内のデータ値が一定でない所定のデータのデータ値を初期値として乱数発生器に供給することにより行われることになる。

【 0 0 2 3 】 即ち、デスクランブル側の乱数発生器には、スクランブルされている第 2 のストリーム部ごとに、値を一定としない初期値が供給されることになるので、乱数発生器から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【 0 0 2 4 】 また、本発明のスクランブル装置は、第 1 のストリーム部の後方に第 2 のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームのうち、スクランブルの対象とされている第 2 のストリーム部をスクランブルするスクランブル装置であって、乱数を発生する乱数発生器と、前記スクランブルの対象とされている第 2 のストリーム部ごとに、前記第 1 のストリーム部内のデータ値が一定でない所定のデータのデータ値を初期値として前記乱数発生器に供給する初

期値供給回路と、前記スクランブルの対象とされている第 2 のストリーム部と前記乱数発生器から出力される乱数とを論理演算して前記スクランブルの対象とされている第 2 のストリーム部をスクランブルする論理演算回路とを備えて備えというものである。

【 0 0 2 5 】 本発明のスクランブル装置を使用する場合には、デスクランブル装置は、乱数を発生する乱数発生器と、スクランブルされている第 2 のストリーム部ごとに、第 1 のストリーム部内のデータ値が一定でない所定のデータのデータ値を初期値として乱数発生器に供給する初期値供給回路と、スクランブルされている第 2 のストリーム部と乱数発生器から出力される乱数とを論理演算してスクランブルされている第 2 のストリーム部をデスクランブルする論理演算回路とを備えて構成されることになる。

【 0 0 2 6 】 即ち、デスクランブル装置の乱数発生器には、スクランブルされている第 2 のストリーム部ごとに、値を一定としない初期値が供給されることになるので、乱数発生器から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【 0 0 2 7 】 また、本発明のデスクランブル方法は、第 1 のストリーム部の後方に第 2 のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームのうち、デスクランブルの対象とされている第 2 のストリーム部を乱数発生器を使用してデスクランブルするデスクランブル方法であって、前記デスクランブルの対象とされている第 2 のストリーム部ごとに、前記第 1 のストリーム部内のデータ値が一定でない所定のデータのデータ値を初期値として前記乱数発生器に供給することにより、前記デスクランブルの対象とされている第 2 のストリーム部をデスクランブルするというものである。

【 0 0 2 8 】 本発明のデスクランブル方法によれば、乱数発生器には、スクランブルされている第 2 のストリーム部ごとに、値を一定としない初期値が供給されることになるので、乱数発生器から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【 0 0 2 9 】 また、本発明のデスクランブル装置は、第 1 のストリーム部の後方に第 2 のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームのうち、デスクランブルの対象とされている第 2 のストリーム部をデスクランブルするデスクランブル装置であって、乱数を発生する乱数発生器と、前記デスクランブルの対象とされている第 2 のストリーム部ごとに、前記第 1 のストリーム部内のデータ値が一定でない所定のデータのデータ値を初期値として前記乱数発生器に供給する初期値供給回路と、前記デスクランブルの対象とされている第 2 のストリーム部と前記乱数発生器から出

力される乱数とを論理演算して前記デスクランブルの対象とされている第2のストリーム部をデスクランブルする論理演算回路とを備えるというものである。

【0030】本発明のデスクランブル装置によれば、乱数発生器には、スクランブルされている第2のストリーム部ごとに、値を一定としない初期値が供給されることになるので、乱数発生器から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【0031】また、本発明のデータ伝達方法は、伝達元において、第1のストリーム部の後方に第2のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームについて、本発明のスクランブル方法を実行し、これにより得られるストリームを伝達メディアを介して伝達先に伝達し、伝達先において本発明のデスクランブル方法を実行し、第1のストリーム部の後方に第2のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームを復元する工程を含むというものである。

【0032】本発明のデータ伝達方法によれば、本発明のスクランブル方法及び本発明のデスクランブル方法を使用しているの、機密性の高いデータ伝達を実現することができる。

【0033】本発明のデータ伝達システムは、本発明のスクランブル装置を有し、第1のストリーム部の後方に第2のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームをスクランブルの対象とされている第2のストリーム部をスクランブルしてなるストリームに変換して伝達メディアに伝達する伝達元と、本発明のデスクランブル装置を有し、伝達メディアから供給されるストリームを第1のストリーム部の後方に第2のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームに復元する伝達先とを備えて構成されるものである。

【0034】本発明のデータ伝達装置によれば、本発明のスクランブル装置及び本発明のデスクランブル装置を使用しているの、機密性の高いデータ伝達を実現することができる。

【0035】

【発明の実施の形態】以下、図1～図11を参照して、本発明のデータ伝達方法及びシステムの実施の第1の形態～第5の形態について、本発明のスクランブル方法及び装置並びに本発明のデスクランブル方法及び装置の実施の形態を含めて説明する。

【0036】第1の形態・・図1～図4

図1は本発明のデータ伝達方法の実施の第1の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第1の形態）の要部を示すブロック図である。

【0037】図1中、20は映像データを得るための力

メラ、21は音声データを得るためのマイク、22はカメラ20により得られる映像データとマイク21により得られる音声データとを符号化して時分割多重し、MPEG2-PS（プログラム・ストリーム）標準に基づくストリームにエンコードするMPEGエンコーダである。

【0038】図2は、MPEG2-PSのPES（Packetized Elementary Stream）パケットの構造を示す図である。図2中、PTS（Presentation Time Stamp）は再生出力の時刻管理情報であり、一般に、700msごとに挿入される。

【0039】また、DTS（Decoding Time Stamp）は復号の時刻管理情報、PESスクランブル制御はスクランブル制御の有無を表示するデータ、PTS&DTSフラグはPTSデータが存在するか否かを示すフラグである。

【0040】また、図1において、23はMPEGエンコーダ22から出力されるストリームをスクランブルの対象とされているパケット・データ部のストリームがスクランブルされてなるストリームに変換するスクランブル回路である。

【0041】このスクランブル回路23は、本発明のスクランブル方法の実施の第1の形態の実施に使用するスクランブル装置であり、本発明のスクランブル装置の実施の第1の形態をなすものである。

【0042】スクランブル回路23において、24は鍵信号により指定される系列の乱数を発生するDES（Data Encryption Standard）規格の乱数発生器、25はMPEGエンコーダ22から出力されるストリームを入力し、パケット開始コードの検出、PESスクランブル制御の内容の確認、PTS&DTSフラグの確認、PTSの位置検出及びパケット・データ部の開始位置検出などを行う位置検出回路である。

【0043】また、26はPTSデータを保持するデータ保持回路であり、このデータ保持回路26は、位置検出回路25がPTSの位置を検出すると、この位置検出したPTSのデータを保持するように位置検出回路25により制御される。

【0044】また、27はデータ保持回路26が保持するPTSデータ又は乱数発生器24から出力される乱数自身を乱数発生器24に供給する選択回路であり、この選択回路27は、位置検出回路25がスクランブルの対象とされているパケット・データ部の開始位置を検出すると、データ保持回路26が保持するPTSデータを初期値として乱数発生器24に供給し、その後、パケット・データ部のストリームが終了するまで、乱数発生器24から出力される乱数をフィードバックするように位置検出回路25により制御される。

【0045】なお、これら位置検出回路25と、データ保持回路26と、選択回路27とでスクランブル回路2

3における初期値供給回路が構成されている。

【0046】また、28はMPEGエンコーダ22から出力されるストリームのうち、スクランブルの対象とされているバケット・データ部のストリームと乱数発生器24から出力される乱数とをEOR処理し、スクランブルの対象とされているバケット・データ部のストリームをスクランブルするEOR回路である。

【0047】また、29はMPEGエンコーダ22から出力されるストリームとEOR回路28から出力されるストリームとを選択して出力する選択回路であり、この選択回路29は、MPEGエンコーダ22から出力されるストリームをスクランブルの対象とされているバケット・データ部のストリームがスクランブルされてなるストリームに変換したストリームを出力するように位置検出回路25により制御される。

【0048】また、30は選択回路29から出力されるストリーム、即ち、スクランブル回路23から出力されるストリームを蓄積するディスク等の蓄積メディア、31は蓄積メディア30から供給されるストリームをスクランブルされているバケット・データ部のストリームがデスクランブルされてなるストリームに変換するデスクランブル回路である。

【0049】このデスクランブル回路31は、本発明のデスクランブル方法の実施の第1の形態の実施に使用するデスクランブル装置であり、本発明のデスクランブル装置の実施の第1の形態をなすものである。

【0050】このデスクランブル回路31において、32は乱数発生器24と同一の回路構成の乱数発生器であり、この乱数発生器32には乱数発生器24に使用された鍵信号と同一内容の鍵信号が供給される。

【0051】また、33は蓄積メディア30から供給されるストリームを入力し、バケット開始コードの検出、PESスクランブル制御の内容の確認、PTS&DTSフラグの確認、PTSの位置検出及びバケット・データ部の開始位置検出などを行う位置検出回路である。

【0052】また、34はPTSデータを保持するデータ保持回路であり、このデータ保持回路34は、位置検出回路33がPTSの位置を検出すると、この位置検出したPTSのデータを保持するように位置検出回路33により制御される。

【0053】また、35はデータ保持回路34が保持するPTSデータ又は乱数発生器32から出力される乱数自身を乱数発生器32に供給する選択回路であり、この選択回路35は、位置検出回路33がデスクランブルの対象、即ち、スクランブルされているバケット・データ部の開始位置を検出すると、データ保持回路34が保持するPTSデータを初期値として乱数発生器32に供給し、その後、バケット・データ部のストリームが終了するまで、乱数発生器32から出力される乱数をフィードバックするように位置検出回路33により制御される。

【0054】なお、これら位置検出回路33と、データ保持回路34と、選択回路35とでデスクランブル回路31における初期値供給回路が構成されている。

【0055】また、36は蓄積メディア30から供給されるストリームのうち、スクランブルされているバケット・データ部のストリームと乱数発生器32から出力される乱数とをEOR処理し、スクランブルされているバケット・データ部のストリームをデスクランブルするEOR回路である。

【0056】また、37は蓄積メディア30から供給されるストリームと、EOR回路36から出力されるストリームとを選択して出力する選択回路であり、この選択回路37は、蓄積メディア30から供給されるストリームをスクランブルされているバケット・データ部のストリームがデスクランブルされてなるストリームに変換したストリームを出力するように位置検出回路33により制御される。

【0057】また、38は選択回路37から出力されるストリーム、即ち、デスクランブル回路31から出力されるストリームから映像データのストリームと音声データのストリームとを分離して復号化するMPEGデコーダ、39はMPEGデコーダ38から出力される映像データ及び音声データが供給されるテレビジョン受像機である。

【0058】このデータ伝達システムにおいては、カメラ20により得られる映像データとマイク21により得られる音声データとは、MPEGエンコーダ22によって、MPEG2-PS標準に基づくストリームにエンコードされ、スクランブル回路23に入力され、位置検出回路25、データ保持回路26、EOR回路28及び選択回路29に供給される。

【0059】図3はスクランブル回路23の動作（本発明のスクランブル方法の実施の第1の形態）を説明するためのフローチャートであり、スクランブル回路23においては、同一動作が繰り返して行われるので、選択回路29からスクランブルの対象とされているバケット・データ部のストリームの出力を終了した時から動作を説明すると、位置検出回路25は、MPEGエンコーダ22から入力されるストリームをそのまま出力し続けるように選択回路29を制御し（ステップS1）、バケット開始コードを検出するための状態となる（ステップS2）。

【0060】そして、位置検出回路25は、バケット開始コードを検出した場合、バケット・ヘッダ部のスクランブル制御の内容からバケット・データ部のストリームがスクランブルの対象であるか否かを判断し（ステップS3）、スクランブルの対象とされていない場合（NOの場合）には、動作はステップS2に戻り、位置検出回路25は、バケット開始コードを検出するための状態となる。

【0061】これに対して、バケット・データ部のストリームがスクランブルの対象とされている場合（ステップS3において、YESの場合）には、位置検出回路25は、バケット・ヘッダ部のPTS&DTSフラグが“10”又は“11”であるか否か、即ち、PTSデータの有無を判断する（ステップS4）。

【0062】判断の結果、PTS&DTSフラグが“10”又は“11”の場合、即ち、PTSデータが存在する場合には、位置検出回路25は、PTSの位置を検出して、PTSデータをデータ保持回路26に保持させ（ステップS5）、バケット・データ部の開始位置を検出するための状態となる（ステップS6）。

【0063】これに対して、PTS&DTSフラグが“10”又は“11”以外の場合、即ち、PTSデータが存在しない場合には、位置検出回路25は、そのまま、バケット・データ部の開始位置を検出するための状態となる（ステップS6）。

【0064】そして、位置検出回路25は、バケット・データ部の開始位置を検出すると、データ保持回路26が保持するPTSデータ、即ち、スクランブルしようとするバケット・データ部と同一のバケットのバケット・ヘッダ部のPTSのデータ、あるいは、スクランブルしようとするバケット・データ部と同一のバケットのバケット・ヘッダ部にPTSが存在しない場合には、PTSが存在するバケット・ヘッダ部のうち、直前のバケット・ヘッダ部のPTSデータを初期値として乱数発生器24に供給するように選択回路27を制御する（ステップS7）。

【0065】ここに、EOR回路28においては、MP EGエンコーダ22から出力されるストリームのうち、スクランブルの対象とされているバケット・データ部のストリームと、乱数発生器24から出力される乱数とがEOR処理され、スクランブルの対象とされているバケット・データ部のストリームのスクランブルが行われる。

【0066】そこで、位置検出回路25は、選択回路29を制御して、EOR回路28から出力されるスクランブルされたストリームを出力し続けさせ（ステップS8）、バケット・データ部のストリームが終了するまで待ち（ステップS9）、ステップS1に戻る。

【0067】このようにして、MPEGエンコーダ22から出力されるストリームは、スクランブルの対象とされているバケット・データ部のストリームがスクランブルされてなるストリームに変換されて蓄積メディア30に蓄積され、この蓄積メディア30に蓄積されたストリームは、適宜、デスクランブル回路31に供給されることになる。

【0068】図4はデスクランブル回路31の動作（本発明のデスクランブル方法の実施の第1の形態）を説明するためのフローチャートであり、デスクランブル回路

31においては、同一動作が繰り返して行われるので、選択回路37からデスクランブルの対象とされているバケット・データ部のストリームの出力を終了した時から動作を説明すると、位置検出回路33は、蓄積メディア30から供給されるストリームをそのまま出力し続けるように選択回路37を制御し（ステップP1）、バケット開始コードを検出するための状態となる（ステップP2）。

【0069】そして、位置検出回路33は、バケット開始コードを検出した場合、バケット・ヘッダ部のスクランブル制御の内容からバケット・データ部のストリームがデスクランブルの対象とされているか否か、即ち、スクランブルされているか否かを判断し（ステップP3）、スクランブルされていない場合（NOの場合）には、動作はステップP2に戻り、位置検出回路33は、バケット開始コードを検出するための状態となる。

【0070】これに対して、バケット・データ部のストリームがスクランブルされている場合（ステップP3において、YESの場合）には、位置検出回路33は、バケット・ヘッダ部のPTS&DTSフラグが“10”又は“11”であるか否か、即ち、PTSデータの有無を判断する（ステップP4）。

【0071】判断の結果、PTS&DTSフラグが“10”又は“11”の場合、即ち、PTSデータが存在する場合には、位置検出回路33は、PTSの位置を検出して、PTSデータをデータ保持回路34に保持させ（ステップP5）、バケット・データ部の開始位置を検出するための状態となる（ステップP6）。

【0072】これに対して、PTS&DTSフラグが“10”又は“11”以外の場合、即ち、PTSデータが存在しない場合には、位置検出回路33は、そのまま、バケット・データ部の開始位置を検出するための状態となる（ステップP6）。

【0073】そして、位置検出回路33は、バケット・データ部の開始位置を検出すると、データ保持回路34が保持するPTSデータ、即ち、デスクランブルしようとするバケット・データ部と同一のバケットのバケット・ヘッダ部のPTSのデータ、あるいは、デスクランブルしようとするバケット・データ部と同一のバケットのバケット・ヘッダ部にPTSが存在しない場合には、PTSが存在するバケット・ヘッダ部のうち、直前のバケット・ヘッダ部のPTSデータを初期値として乱数発生器32に供給するように選択回路35を制御する（ステップP7）。

【0074】ここに、EOR回路36では、蓄積メディア30から供給されるストリームのうち、スクランブルされているバケット・データ部のストリームと、乱数発生器32から出力される乱数とがEOR処理され、スクランブルされているバケット・データ部のストリームのデスクランブルが行われる。



【0075】そこで、位置検出回路33は、選択回路37を制御し、EOR回路36から出力されるデスクランブルされたストリームを出力し続けさせ(ステップP8)、パケット・データ部のストリームが終了するまで待ち(ステップP9)、ステップP1に戻る。

【0076】このようにして、蓄積メディア30から供給されるストリームは、スクランブルされているパケット・データ部のストリームがデスクランブルされてなるストリームに変換され、MPEGデコーダ38に伝達される。

【0077】MPEGデコーダ38においては、デスクランブル回路31から伝達されるストリームから映像データのストリームと音声データのストリームとが分離されて復号化され、これら復号化された映像データ及び音声データは、テレビジョン受信機39に伝達される。

【0078】このように、本発明のデータ伝達方法及びシステムの実施の第1の形態においては、MPEGエンコーダ22から出力されるMPEG2-PS標準のストリームは、スクランブル回路23において、スクランブルの対象とされているパケット・データ部のストリームをスクランブルしてなるストリームに変換され、蓄積メディア30を介して、デスクランブル回路31に供給され、デスクランブルが行われて、MPEGデコーダ38に伝達される。

【0079】ここに、スクランブル回路23においては、スクランブルの対象とされているパケット・データ部のストリームごとに、スクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部のPTSのデータ、あるいは、スクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部にPTSが存在しない場合には、PTSが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のPTSのデータ値を初期値として乱数発生器24に供給することにより、スクランブルの対象とされているパケット・データ部のストリームのスクランブルが行われる。

【0080】この結果、デスクランブル回路31においては、スクランブルされているパケット・データ部のストリームごとに、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部のPTSのデータ、あるいは、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部にPTSが存在しない場合には、PTSが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のPTSのデータ値を初期値として乱数発生器32に供給することにより、スクランブルされているパケット・データ部のストリームのデスクランブルが行われることになる。

【0081】このように、本発明のデータ伝達方法及びシステムの実施の第1の形態によれば、デスクランブル

回路31の乱数発生器32には、スクランブルされているパケット・データ部のストリームごとに、データ値を一定としないPTSのデータ値が初期値として供給されることになるので、乱数発生器32から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【0082】第2の形態・図5～図8

図5は本発明のデータ伝達方法の実施の第2の形態の実施に使用するデータ伝達システム(本発明のデータ伝達システムの実施の第2の形態)の要部を示すブロック図である。

【0083】図5中、41は映像データを得るためのカメラ、42は音声データを得るためのマイク、43はカメラ41により得られる映像データとマイク42により得られる音声データとを符号化して時分割多重し、MPEG2-TS(トランスポート・ストリーム)標準に基づくストリームにエンコードするMPEGエンコーダである。

【0084】図6はMPEG2-TSのトランスポート・パケットの構造を示す図であり、PCR(Program Clock Reference)はMPEGデコーダにおいて、時刻標準となるSTC(基本となる同期信号)の値をMPEGエンコーダ43で意図した値にセット・校正するための情報である。なお、PCRは、一般に、100msごとに挿入される。

【0085】また、アダプテーションフラグはアダプテーション・フィールドの有無を示すフラグ、ペイロードフラグはペイロードの有無を示すフラグ、PCRフラグはPCRがあるか否かを示すフラグである。

【0086】また、図5において、44はMPEGエンコーダ43から出力されるストリームをスクランブルの対象とされているペイロード部のストリームがスクランブルされてなるストリームに変換するスクランブル回路である。

【0087】このスクランブル回路44は、本発明のスクランブル方法の実施の第2の形態の実施に使用するスクランブル装置であり、本発明のスクランブル装置の実施の第2の形態をなすものである。

【0088】スクランブル回路44において、45は鍵信号により指定される系列の乱数を発生するDES規格の乱数発生器、46はMPEGエンコーダ43から出力されるストリームに含まれている同期バイトの検出、アダプテーションフラグの内容の確認、ペイロードフラグの内容の確認、PCRフラグの内容の確認、PCRの位置検出及びペイロード部の開始位置検出などを行う位置検出回路である。

【0089】また、47はPCRデータを保持するデータ保持回路であり、このデータ保持回路47は、位置検出回路46がPCRの位置を検出すると、この位置検出したPCRのデータを保持するように位置検出回路46

により制御される。

【0090】また、48はデータ保持回路47が保持するPCRデータ又は乱数発生器45から出力される乱数自身を乱数発生器45に供給する選択回路であり、この選択回路48は、位置検出回路46がスクランブルの対象のペイロード部の開始位置を検出すると、データ保持回路47が保持するPCRデータを初期値として乱数発生器45に供給し、その後、ペイロード部のストリームが終了するまで、乱数発生器45から出力される乱数をフィードバックするように位置検出回路46により制御される。

【0091】なお、これら位置検出回路46と、データ保持回路47と、選択回路48とでスクランブル回路44における初期値供給回路が構成されている。

【0092】また、49はMPEGエンコーダ43から出力されるストリームのうち、スクランブルの対象とされているペイロード部のストリームと乱数発生器45から出力される乱数とをEOR処理し、スクランブルの対象とされているペイロード部のストリームをスクランブルするEOR回路である。

【0093】また、50はMPEGエンコーダ43から出力されるストリームとEOR回路49から出力されるストリームとを選択して出力する選択回路であり、この選択回路50は、MPEGエンコーダ43から出力されるストリームをスクランブルの対象とされているペイロード部のストリームがスクランブルされてなるストリームに変換したストリームを出力するように位置検出回路46により制御される。

【0094】また、51は選択回路50から出力されるストリーム、即ち、スクランブル回路44から出力されるストリームをデジタル変調するデジタル変調器、52はデジタル変調器51の出力を送信するためのアップ・コンバータ、53は送信側のアンテナである。

【0095】また、54は受信側のアンテナ、55は選局を行うチューナ、56はチューナ55によって選局した信号をデジタル復調するデジタル復調器である。

【0096】また、57はデジタル復調器56から出力されるストリームをスクランブルされているペイロード部のストリームをデスクランブルしたストリームに変換するデスクランブル回路である。

【0097】このデスクランブル回路57は、本発明のデスクランブル方法の実施の第2の形態の実施に使用するデスクランブル装置であり、本発明のデスクランブル装置の実施の第2の形態をなすものである。

【0098】デスクランブル回路57において、58は乱数発生器45と同一の回路構成の乱数発生器であり、この乱数発生器58には乱数発生器45に使用された鍵信号と同一内容の鍵信号が供給される。

【0099】また、59はデジタル復調器56から出力されるストリームに含まれている同期バイトの検出、

アダプテーションフラグの内容の確認、ペイロードフラグの内容の確認、PCRフラグの内容の確認、PCRの位置検出及びペイロード部の開始位置検出などを行う位置検出回路である。

【0100】また、60はPCRデータを保持するデータ保持回路であり、このデータ保持回路60は、位置検出回路59がPCRの位置を検出すると、この位置検出したPCRのデータを保持するように位置検出回路59により制御される。

【0101】また、61はデータ保持回路60が保持するPCRデータ又は乱数発生器58から出力される乱数自身を乱数発生器58に供給する選択回路であり、この選択回路61は、位置検出回路59がデスクランブルの対象、即ち、スクランブルされているペイロード部の位置を検出すると、データ保持回路60が保持するPCRデータを初期値として乱数発生器58に供給し、その後、ペイロード部のストリームが終了するまで、乱数発生器58から出力される乱数をフィードバックするように位置検出回路59により制御される。

【0102】なお、これら位置検出回路59と、データ保持回路60と、選択回路61とでデスクランブル回路57における初期値供給回路が構成されている。

【0103】また、62はデジタル復調器56から入力されるストリームのうち、スクランブルされているペイロード部のストリームと乱数発生器58から出力される乱数とをEOR処理し、スクランブルされているペイロード部のストリームをデスクランブルするEOR回路である。

【0104】また、63はデジタル復調器56から出力されるストリームと、EOR回路62から出力されるストリームとを選択して出力する選択回路であり、この選択回路63は、デジタル復調器56から出力されるストリームをスクランブルされているペイロード部のストリームがデスクランブルされてなるストリームに変換したストリームを出力するように位置検出回路59により制御される。

【0105】また、64は選択回路63から出力されるストリーム、即ち、デスクランブル回路57から出力されるストリームから映像データのストリームと音声データのストリームとを分離して復号化するMPEGデコーダ、65はMPEGデコーダ64から出力される映像データ及び音声データが供給されるテレビジョン受像機である。

【0106】このデータ伝達システムにおいては、カメラ41により得られる映像データとマイク42により得られる音声データとは、MPEGエンコーダ43によって、MPEG2-TS標準に基づくストリームにエンコードされてスクランブル回路44に入力され、位置検出回路46、データ保持回路47、EOR回路49及び選択回路50に供給される。

【0107】図7はスクランブル回路44の動作（本発明のスクランブル方法の実施の第2の形態）を説明するためのフローチャートであり、スクランブル回路44においては、同一動作が繰り返して行われるので、選択回路50からスクランブルの対象とされているペイロード部のストリームの出力を終了した時から動作を説明すると、位置検出回路46は、MPEGエンコーダ43から入力されるストリームをそのまま出力し続けるように選択回路50を制御し、同期バイトを検出するための状態となる（ステップN1）。

【0108】そして、位置検出回路46は、同期バイトを検出した場合、パケット・ヘッダ部のスクランブル制御の内容からペイロード部のストリームがスクランブルの対象とされているか否かを判断し（ステップN2）、スクランブルの対象とされていない場合（NOの場合）には、動作はステップN1に戻り、位置検出回路46は、同期バイトを検出するための状態となる。

【0109】これに対して、ペイロード部のストリームがスクランブルの対象とされている場合（ステップN3において、YESの場合）には、位置検出回路46は、アダプテーション・フラグからアダプテーション・フィールドがあるか否かを判断する（ステップN3）。

【0110】判断の結果、アダプテーション・フィールドがある場合（YESの場合）には、位置検出回路46は、PCRフラグからPCRがあるか否かを判断し（ステップN4）、PCRがある場合（YESの場合）には、PCRの位置を検出し、PCRデータをデータ保持回路47に保持させる（ステップN5）。

【0111】そして、位置検出回路46は、ペイロードフラグからペイロードがあるか否かを判断し（ステップN6）、ペイロードがある場合（YESの場合）には、ペイロード部の開始位置を検出するまで待ち（ステップN7）、ペイロードがない場合（NOの場合）には、動作はステップN1に戻る。

【0112】ここに、ステップN3において、アダプテーション・フィールドがないと判断した場合（NOの場合）や、ステップN4において、PCRがないと判断した場合（NOの場合）、動作はステップN6に移行する。

【0113】そして、ステップN7の後、位置検出回路46は、ペイロード部の開始位置を検出すると、データ保持回路47が保持するPCRデータ、即ち、スクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部のPCRのデータ、あるいは、スクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部にPCRが存在しない場合には、PCRが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のPCRデータを初期値として乱数発生器45に供給するように選択回路48を制御する（ステップN8）。

【0114】ここに、EOR回路49においては、MPEGエンコーダ43から入力されるストリームのうち、スクランブルの対象とされているペイロード部のストリームと、乱数発生器45から出力される乱数とをEOR処理し、スクランブルの対象とされているペイロード部のスクランブルが行われる。

【0115】そして、位置検出回路46は、選択回路50を制御して、EOR回路49から出力されるスクランブルされたストリームを出力し続けさせ（ステップN9）、ペイロード部のストリームが終了するまで待ち（ステップN10）、ステップN1に戻る。

【0116】このようにして、MPEGエンコーダ43から出力されるストリームは、スクランブルの対象とされているペイロード部のストリームがスクランブルされてなるストリームに変換され、デジタル変調器51、アップコンバータ52、アンテナ53、54、チューナ55及びデジタル復調器56を介してデスクランブル回路57に伝達される。

【0117】図8はデスクランブル回路57の動作（本発明のデスクランブル方法の実施の第2の形態）を説明するためのフローチャートであり、デスクランブル回路57においては、同一動作が繰り返して行われるので、選択回路63からデスクランブルの対象とされているペイロード部、即ち、スクランブルされているペイロード部のストリームの出力を終了した時から動作を説明すると、位置検出回路59は、デジタル復調器56から入力されるストリームをそのまま出力し続けるように選択回路63を制御し、同期バイトを検出するための状態となる（ステップQ1）。

【0118】そして、位置検出回路59は、同期バイトを検出した場合、パケット・ヘッダ部のスクランブル制御の内容からペイロード部のストリームがデスクランブルの対象、即ち、スクランブルされているか否かを判断し（ステップQ2）、スクランブルされていない場合（NOの場合）には、動作はステップQ1に戻り、位置検出回路46は、同期バイトを検出するための状態となる。

【0119】これに対して、ペイロード部のストリームがスクランブルの対象とされている場合（ステップQ2において、YESの場合）には、位置検出回路59は、アダプテーション・フラグからアダプテーション・フィールドがあるか否かを判断する（ステップQ3）。

【0120】判断の結果、アダプテーション・フィールドがある場合（YESの場合）には、位置検出回路59は、PCRフラグからPCRがあるか否かを判断し（ステップQ4）、PCRがある場合（YESの場合）には、PCRの位置を検出し、PCRデータをデータ保持回路60に保持させる（ステップQ5）。

【0121】そして、位置検出回路59は、ペイロードフラグからペイロードがあるか否かを判断し（ステップ

21

Q 6)、ペイロードがある場合 (YES の場合) には、ペイロード部の開始位置を検出するまで待ち (ステップ Q 7)、ペイロードがない場合 (NO の場合) には、動作はステップ Q 1 に戻る。

【0122】ここに、ステップ Q 3 において、アダプテーション・フィールドがないと判断した場合 (NO の場合) や、ステップ Q 4 において、PCR がないと判断した場合 (NO の場合)、動作はステップ Q 6 に移行する。

【0123】そして、ステップ Q 7 の後、位置検出回路 5 9 は、ペイロード部の開始位置を検出すると、データ保持回路 6 0 が保持する PCR データ、即ち、デスクランブルしようとするペイロード部と同一のバケットのバケット・ヘッダ部の PCR のデータ、あるいは、デスクランブルしようとするペイロード部と同一のバケットのバケット・ヘッダ部に PCR が存在しない場合には、PCR が存在するバケット・ヘッダ部のうち、直前のバケット・ヘッダ部の PCR データを初期値として乱数発生器 5 8 に供給するように選択回路 6 1 を制御する (ステップ Q 8)。

【0124】ここに、EOR 回路 6 2 においては、ディジタル復調器 5 6 から入力されるストリームのうち、スクランブルされているペイロード部のストリームと、乱数発生器 5 8 から出力される乱数とを EOR 処理し、スクランブルされているペイロード部のデスクランブルが行われる。

【0125】そして、位置検出回路 5 9 は、選択回路 6 3 を制御して、EOR 回路 6 2 から出力されるデスクランブルされたストリームを出力し続けさせ (ステップ Q 9)、ペイロード部のストリームが終了するまで待ち (ステップ Q 10)、ステップ Q 1 に戻る。

【0126】このようにして、ディジタル復調器 5 6 から出力されるストリームは、デスクランブル回路 5 7 において、スクランブルされているペイロード部のストリームがデスクランブルされてなるストリームに変換され、MPEG デコーダ 6 4 に伝達される。

【0127】MPEG デコーダ 6 4 においては、デスクランブル回路 5 7 から伝達されるストリームから映像データのストリームと音声データのストリームとが分離されて復号化され、これら復号化された映像データ及び音声データは、テレビジョン受像機 6 5 に伝達される。

【0128】このように、本発明のデータ伝達方法及びシステムの実施の第 2 の形態においては、MPEG エンコーダ 4 3 から出力される MPEG 2-TS 標準のストリームは、スクランブル回路 4 4 において、スクランブルの対象とされているペイロード部のストリームをスクランブルしてなるストリームに変換され、デスクランブル回路 5 7 に供給され、デスクランブルが行われて、MPEG デコーダ 6 4 に伝達される。

【0129】ここに、スクランブル回路 4 4 において

22

は、スクランブルの対象とされているペイロード部のストリームごとに、スクランブルしようとするペイロード部と同一のバケットのバケット・ヘッダ部の PCR のデータ、あるいは、スクランブルしようとするペイロード部と同一のバケットのバケット・ヘッダ部に PCR が存在しない場合には、PCR が存在するバケット・ヘッダ部のうち、直前のバケット・ヘッダ部の PCR のデータ値を初期値として乱数発生器 4 5 に供給することにより、スクランブルの対象とされているペイロード部のストリームのスクランブルが行われる。

【0130】この結果、デスクランブル回路 5 7 においては、スクランブルされているペイロード部のストリームごとに、デスクランブルしようとするペイロード部と同一のバケットのバケット・ヘッダ部の PCR のデータ、あるいは、デスクランブルしようとするペイロード部と同一のバケットのバケット・ヘッダ部に PCR が存在しない場合には、PCR が存在するバケット・ヘッダ部のうち、直前のバケット・ヘッダ部の PCR のデータ値を初期値として乱数発生器 5 8 に供給することにより、スクランブルされているペイロード部のストリームのデスクランブルが行われることになる。

【0131】このように、本発明のデータ伝達方法及びシステムの実施の第 2 の形態によれば、デスクランブル回路 5 7 の乱数発生器 5 8 には、スクランブルされているペイロード部のストリームごとに、データ値を一定としない PCR のデータ値が初期値として供給されることになるので、乱数発生器 5 8 から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【0132】なお、この例では、PCR のデータ値を初期値として乱数発生器 4 5、5 8 に供給するようにした場合について説明したが、この代わりに、たとえば、巡回カウンタのデータ値又は PCR と巡回カウンタとを組み合わせ又は演算したデータのデータ値を乱数発生器 4 5、5 8 に供給するようにしても良い。

【0133】第 3 の形態・図 9

図 9 は本発明のデータ伝達方法の実施の第 3 の形態の実施に使用するデータ伝達システム (本発明のデータ伝達システムの実施の第 3 の形態) の要部を示すブロック図である。

【0134】図 9 中、6 7 は映像データを得るためのカメラ、6 8 は音声データを得るためのマイク、6 9 はカメラ 6 7 により得られる映像データとマイク 6 8 により得られる音声データとを符号化して時分割多重し、MPEG 2-PS 標準に基づくストリームにエンコードする MPEG エンコーダである。

【0135】また、7 0 は MPEG エンコーダ 6 9 から出力されるストリームをスクランブルの対象とされているバケット・データ部のストリームがスクランブルされてなるストリームに変換するスクランブル回路である。

【0136】このスクランブル回路70は、本発明のスクランブル方法の実施の第3の形態の実施に使用するスクランブル装置であり、本発明のスクランブル装置の実施の第3の形態をなすものである。

【0137】スクランブル回路70において、71は鍵信号により指定される系列の乱数を発生するDES規格の乱数発生器、72はMPEGエンコーダ69から入力されるストリームを入力し、パケット開始コードの検出、PESスクランブル制御の内容の確認、PTS&DTSフラグの内容の確認、PTSの位置検出及びパケット・データ部の開始位置検出などを行う位置検出回路である。

【0138】また、73はMPEGエンコーダ69から入力されるストリームを64ビットの並列ストリームにパラレル変換するシリアル/パラレル変換回路(S/P)、74はPTSデータを保持する40ビット構成のレジスタ(RS)であり、このレジスタ74は、位置検出回路72がPTSの位置を検出すると、シリアル/パラレル変換回路73から出力されるPTSデータを保持するように位置検出回路72により制御される。

【0139】また、75は位置検出回路72に制御され、シリアル/パラレル変換回路73から出力されるストリームのうち、スクランブルの対象とされているパケット・データ部のストリームを保持する64ビット構成のレジスタである。

【0140】また、76はレジスタ74が保持するPTSデータ又は乱数発生器71から出力される乱数自身を乱数発生器71に供給する選択回路であり、この選択回路76は、位置検出回路72がスクランブルの対象とされているパケット・データ部の開始位置を検出すると、レジスタ74が保持するPTSデータを初期値として乱数発生器71に供給し、その後、パケット・データ部のストリームが終了するまで、乱数発生器71から出力される乱数をフィードバックするように位置検出回路72により制御される。

【0141】なお、位置検出回路72と、レジスタ74と、選択回路76とでスクランブル回路70における初期値供給回路が構成されている。

【0142】また、77はレジスタ75から出力される並列ストリームのストリームと乱数発生器71から出力される乱数とをEOR処理し、スクランブルの対象とされているパケット・データ部のストリームをスクランブルするEOR回路である。

【0143】また、78は位置検出回路72に制御され、EOR回路77から出力される並列ストリームを保持する64ビット構成のレジスタ、79はレジスタ78から出力される並列ストリームをシリアル変換するパラレル/シリアル変換回路(P/S)である。

【0144】また、80はMPEGエンコーダ69から入力されるストリームとパラレル/シリアル変換回路7

9から出力されるストリームとを選択して出力する選択回路であり、この選択回路80は、MPEGエンコーダ69から入力されるストリームをスクランブルの対象とされているパケット・データ部のストリームがスクランブルされてなるストリームに変換したストリームを出力するように位置検出回路72により制御される。

【0145】また、81は選択回路80から出力されるストリーム、即ち、スクランブル回路70から出力されるストリームを蓄積するディスク等の蓄積メディア、82は蓄積メディア81から供給されるストリームをスクランブルされているパケット・データ部のストリームをデスクランブルしたストリームに変換するデスクランブル回路である。

【0146】このデスクランブル回路82は、本発明のデスクランブル方法の実施の第3の形態の実施に使用するデスクランブル装置であり、本発明のデスクランブル装置の実施の第3の形態をなすものである。

【0147】デスクランブル回路82において、83は乱数発生器71と同一の回路構成の乱数発生器であり、この乱数発生器83には乱数発生器71に使用された鍵信号と同一内容の鍵信号が供給される。

【0148】また、84は蓄積メディア81から供給されるストリームを入力し、パケット開始コードの検出、PESスクランブル制御の内容の確認、PTS&DTSフラグの内容の確認、PTSの位置検出及びパケット・データ部の開始位置検出などを行う位置検出回路である。

【0149】また、85は蓄積メディア81から供給されるストリームを64ビットの並列ストリームにパラレル変換するシリアル/パラレル変換回路、86はPTSデータを保持する40ビット構成のレジスタであり、このレジスタ86は、位置検出回路84がPTSの位置を検出すると、シリアル/パラレル変換回路85から出力されるPTSデータを保持するように位置検出回路84により制御される。

【0150】また、87は位置検出回路84に制御され、シリアル/パラレル変換回路85から出力されるスクランブルされているパケット・データ部のストリームを保持する64ビット構成のレジスタである。

【0151】また、88はレジスタ86が保持するPTSデータ又は乱数発生器83から出力される乱数自身を乱数発生器83に供給する選択回路であり、この選択回路88は、位置検出回路84がデスクランブルの対象、即ち、スクランブルされているパケット・データ部の開始位置を検出すると、レジスタ86が保持するPTSデータを初期値として乱数発生器83に供給し、その後、パケット・データ部のストリームが終了するまで、乱数発生器83から出力される乱数をフィードバックするように位置検出回路84により制御される。

【0152】なお、位置検出回路84と、レジスタ86

25

と、選択回路 8 8 とでデスクランブル回路 8 2 における初期値供給回路が構成されている。

【0153】また、89 はレジスタ 8 7 から出力される並列ストリームと乱数発生器 8 3 から出力される乱数とを EOR 処理し、スクランブルされているパケット・データ部のストリームをデスクランブルする EOR 回路である。

【0154】また、90 は位置検出回路 8 4 に制御されて、EOR 回路 8 9 から出力される並列ストリームを保持する 6 4 ビット構成のレジスタ、91 はレジスタ 9 0 から出力される並列ストリームをシリアル変換するパラレル／シリアル変換回路である。

【0155】また、92 は蓄積メディア 8 1 から供給されるストリームとパラレル／シリアル変換回路 9 1 から出力されるストリームとを選択して出力する選択回路であり、この選択回路 9 2 は、蓄積メディア 8 1 から供給されるストリームをスクランブルされているパケット・データ部のストリームがデスクランブルされてなるストリームに変換したストリームを出力するように位置検出回路 8 4 により制御される。

【0156】また、93 はデスクランブル回路 8 2 から出力されるストリームから映像データのストリームと音声データのストリームとを分離して復号化する MPEG デコーダ、94 は MPEG デコーダ 9 3 から出力される映像データ及び音声データが供給されるテレビジョン受像機である。

【0157】このデータ伝達システムにおいては、カメラ 6 7 により得られる映像データとマイク 6 8 により得られる音声データとは、MPEG エンコーダ 6 9 によって、MPEG 2 - P S 標準に基づくストリームにエンコードされ、スクランブル回路 7 0 に入力され、位置検出回路 7 2、シリアル／パラレル変換回路 7 3 及び選択回路 8 0 に供給される。

【0158】ここに、位置検出回路 7 2 は、パケット開始コードを検出した場合、パケット・ヘッダ部のスクランブル制御の内容からパケット・データ部のストリームがスクランブルの対象であるか否かを判断し、スクランブルの対象とされていない場合には、パケット開始コードを検出するための状態に戻る。

【0159】これに対して、パケット・データ部のストリームがスクランブルの対象とされている場合には、位置検出回路 7 2 は、パケット・ヘッダ部の P T S & D T S フラグが“10”又は“11”であるか否か、即ち、P T S の有無を判断する。

【0160】判断の結果、P T S & D T S フラグが“10”又は“11”の場合、即ち、P T S が存在する場合には、位置検出回路 7 2 は、P T S の位置を検出して、P T S データをレジスタ 7 4 に保持させ、パケット・データ部の開始位置を検出するための状態となる。

【0161】これに対して、P T S & D T S フラグが

26

“10”又は“11”以外の場合、即ち、P T S が存在しない場合には、位置検出回路 7 2 は、そのまま、パケット・データ部の開始位置を検出するための状態となる。

【0162】そして、位置検出回路 7 2 は、パケット・データ部の開始位置を検出すると、レジスタ 7 4 が保持する P T S データ、即ち、スクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部の P T S のデータ、あるいは、スクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部に P T S が存在しない場合には、P T S が存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部の P T S データを初期値として乱数発生器 7 1 に供給するように選択回路 7 6 を制御すると共に、シリアル／パラレル変換回路 7 3 から出力されるストリームをレジスタ 7 5 に保持させる。

【0163】ここに、EOR 回路 7 7 においては、レジスタ 7 5 から出力されるストリームと乱数発生器 7 1 から出力される乱数とを EOR 処理し、スクランブルの対象とされているパケット・データ部のストリームのスクランブルが行われ、その結果がレジスタ 7 8 に保持され、更に、レジスタ 7 8 から出力される並列ストリームがパラレル／シリアル変換回路 7 9 によりシリアル変換される。

【0164】また、位置検出回路 7 2 は、選択回路 8 0 を制御し、パラレル／シリアル変換回路 7 9 から出力されるストリームを出力し続けさせ、パケット・データ部のストリームが終了するまで待ち、MPEG エンコーダ 6 9 から入力されるストリームをそのまま出力するように選択回路 8 0 を制御する。

【0165】このようにして、MPEG エンコーダ 6 9 から出力されるストリームは、スクランブルの対象とされているパケット・データ部のストリームがスクランブルされてなるストリームに変換されて蓄積メディア 8 1 に蓄積される。

【0166】そして、蓄積メディア 8 1 に蓄積されたストリームは、適宜、デスクランブル回路 8 2 に供給され、位置検出回路 8 4、シリアル／パラレル変換回路 8 5 及び選択回路 9 2 に供給される。

【0167】ここに、位置検出回路 8 4 は、パケット開始コードを検出した場合、パケット・ヘッダ部のスクランブル制御の内容からパケット・データ部のストリームがデスクランブルの対象、即ち、スクランブルされているか否かを判断し、スクランブルされていない場合には、パケット開始コードを検出するための状態に戻る。

【0168】これに対して、パケット・データ部のストリームがスクランブルされている場合には、位置検出回路 8 4 は、パケット・ヘッダ部の P T S & D T S フラグが“10”又は“11”であるか否か、即ち、P T S の有無を判断する。

【0169】判断の結果、PTS&DTSフラグが“10”又は“11”の場合、即ち、PTSが存在する場合には、位置検出回路84は、PTSの位置を検出して、PTSデータをレジスタ86に保持させ、パケット・データ部の開始位置を検出するための状態となる。

【0170】これに対して、PTS&DTSフラグが“10”又は“11”以外の場合、即ち、PTSが存在しない場合には、位置検出回路84は、そのまま、パケット・データ部の開始位置を検出するための状態となる。

【0171】そして、位置検出回路84は、パケット・データ部の開始位置を検出すると、レジスタ86が保持するPTSデータ、即ち、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部のPTSのデータ、あるいは、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部にPTSが存在しない場合には、PTSが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のPTSデータを初期値として乱数発生器83に供給するように選択回路88を制御すると共に、シリアル/パラレル変換回路85から出力されるストリームをレジスタ87に保持させる。

【0172】ここに、EOR回路89においては、レジスタ87から出力されるストリームと乱数発生器83から出力される乱数とをEOR処理し、スクランブルされているパケット・データ部のストリームのスクランブルが行われ、その結果がレジスタ90に保持され、更に、レジスタ90から出力される並列ストリームがパラレル/シリアル変換回路91によりシリアル変換される。

【0173】また、位置検出回路84は、選択回路92を制御し、パラレル/シリアル変換回路91から出力されるストリームを出力し続けさせ、パケット・データ部のストリームが終了するまで待ち、その後、蓄積メディア81から供給されるストリームをそのまま出力するように選択回路92を制御する。

【0174】このようにして、蓄積メディア81から供給されるストリームは、スクランブルされているパケット・データ部のストリームがデスクランブルされてなるストリームに変換され、MPEGデコーダ93に伝達される。

【0175】MPEGデコーダ93においては、デスクランブル回路82から出力されるストリームから映像データのストリームと音声データのストリームとが分離されて復号化され、テレビジョン受信機94に伝達される。

【0176】このように、本発明のデータ伝達方法及びシステムの実施の第3の形態においては、MPEGエンコーダ69から出力されるMPEG2-PS標準のストリームは、スクランブル回路70において、スクランブルの対象とされているパケット・データ部のストリーム

をスクランブルしてなるストリームに変換され、蓄積メディア81を介して、デスクランブル回路82に供給され、デスクランブルが行われて、MPEGデコーダ93に伝達される。

【0177】ここに、スクランブル回路70においては、ストリームを64ビットの並列ストリームに変換し、スクランブルの対象とされているパケット・データ部のストリームごとに、スクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部のPTSのデータ、あるいは、スクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部にPTSが存在しない場合には、PTSが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のPTSのデータ値を初期値として乱数発生器71に供給することにより、スクランブルの対象とされているパケット・データ部のストリームのスクランブルが行われる。

【0178】この結果、デスクランブル回路82においては、ストリームを64ビットの並列ストリームに変換し、スクランブルされているパケット・データ部のストリームごとに、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部のPTSのデータ、あるいは、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部にPTSが存在しない場合には、PTSが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のPTSのデータ値を初期値として乱数発生器83に供給することにより、スクランブルされているパケット・データ部のストリームのデスクランブルが行われることになる。

【0179】このように、本発明のデータ伝達方法及びシステムの実施の第3の形態によれば、デスクランブル回路82の乱数発生器83には、スクランブルされているパケット・データ部のストリームごとに、データ値を一定としないPTSのデータ値が初期値として供給されると共に、乱数発生器83から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【0180】第4の形態・・図10

図10は本発明のデータ伝達方法の実施の第4の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第4の形態）の要部を示すブロック図である。

【0181】図10中、97はパーソナル・コンピュータ、98はデスクランブル回路の一部を構成するPCカード標準リリース2.0に準拠するPCMCIA（Personal Computer Memory Card International Association）カードである。

【0182】ここに、パーソナル・コンピュータ97に

において、99はCPU (Central Processing unit)、100は記憶回路、101はバス、102はPCMCIAインタフェースである。

【0183】また、103はディスク装置であり、104は図1に示すスクランブル回路23から出力されるストリーム、即ち、MPEG2-PS標準のストリームをスクランブルの対象とされているバケット・データ部のストリームをスクランブルしてなるストリームが格納されたディスク、105はディスク104からストリームを読み取るためのディスク読取り機構である。

【0184】また、106はディスク読取り機構105から読み出されたストリームを入力し、バケット開始コードの検出、PESスクランブル制御の内容の確認、PTS&DTSフラグの内容の確認、PTSの位置検出及びバケット・データ部の開始位置検出などを行う位置検出回路である。

【0185】また、PCMCIAカード98において、107は鍵信号が指定する系列の乱数を発生する乱数発生器、108はPTSデータを保持するデータ保持回路であり、このデータ保持回路108は、位置検出回路106がPTSの位置を検出すると、この位置検出したPTSのデータを保持するように位置検出回路106により制御される。

【0186】また、109はデータ保持回路108が保持するPTSデータ又は乱数発生器107から出力される乱数自身を乱数発生器107に供給する選択回路であり、この選択回路109は、位置検出回路106がデスクランブルの対象、即ち、スクランブルされているバケット・データ部の開始位置を検出すると、データ保持回路108が保持するPTSデータを初期値として乱数発生器107に供給し、その後、バケット・データ部のストリームが終了するまで、乱数発生器107から出力される乱数をフィードバックするように位置検出回路106により制御される。

【0187】また、110はディスク読取り機構105から供給されるストリームのうち、スクランブルされているバケット・データ部のストリームと乱数発生器107から出力される乱数とをEOR処理し、スクランブルされているバケット・データ部のストリームをデスクランブルするEOR回路である。

【0188】また、111はディスク読取り機構105から供給されるストリームとEOR回路110から出力されるストリームとを選択して出力する選択回路であり、この選択回路111は、ディスク読取り機構105から供給されるストリームをスクランブルされているバケット・データ部のストリームがデスクランブルされてなるストリームに変換したストリームを出力するように位置検出回路106により制御される。

【0189】また、112はIDデータ (身分証明データ) 等を記憶する記憶回路、113は記憶回路112か

らIDデータを出力する等の処理を行うための処理回路である。

【0190】ここに、位置検出回路106とPCMCIAカード98とでデスクランブル回路が構成されているが、このデスクランブル回路は、本発明のデスクランブル装置の実施の第4の形態をなすものである。

【0191】また、位置検出回路106と、データ保持回路108と、選択回路109とで、デスクランブル回路における初期値供給回路が構成されている。なお、位置検出回路106は、PCMCIAカード98内に設けるようにしても良いが、この例のように、パーソナル・コンピュータ97側に設ける場合には、PCMCIAカード98の入出力端子を減らすことができる。

【0192】また、パーソナル・コンピュータ97において、114は選択回路111から出力されるストリーム、即ち、PCMCIAカード98から出力されるストリームから映像データのストリームと音声データのストリームとを分離して復号化するMPEGデコーダである。

【0193】また、115はMPEGデコーダ114から出力される映像データが供給されるディスプレイ、116はMPEGデコーダ114から出力される音声データが供給されるスピーカである。

【0194】このデータ伝達システムにおいては、パーソナル・コンピュータ97にPCMCIAカード98が入力されると、CPU99は、PCMCIAカード98からIDデータを出力させて、IDデータを認証することができるか否かを判断し、認証することができる場合には、処理回路113に対してスクランブル回路において使用した鍵信号と同一内容の鍵信号を生成させ、乱数発生器107がスクランブル回路における乱数発生器と同一の系列の乱数を発生させることができるようにする。

【0195】そして、ディスク装置103が起動されると、ディスク104に記憶されているストリームがディスク読出し機構105から出力され、位置検出回路106、PCMCIAカード98のデータ保持回路108、EOR回路110及び選択回路111に供給される。

【0196】ここに、位置検出回路106は、バケット開始コードを検出した場合、バケット・ヘッダ部のスクランブル制御の内容からバケット・データ部のストリームがスクランブルされているか否かを判断し、スクランブルされていない場合には、バケット開始コードを検出するための状態に戻る。

【0197】これに対して、バケット・データ部のストリームがスクランブルされている場合には、位置検出回路106は、バケット・ヘッダ部のPTS&DTSフラグが“10”又は“11”であるか否か、即ち、PTSの有無を判断する。

10

20

30

40

50



【0198】判断の結果、PTS&DTSフラグが“10”又は“11”の場合、即ち、PTSが存在する場合には、位置検出回路106は、PTSの位置を検出して、PTSデータをデータ保持回路108に保持させ、バケット・データ部の開始位置を検出するための状態となる。

【0199】これに対して、PTS&DTSフラグが“10”又は“11”以外の場合、即ち、PTSが存在しない場合には、位置検出回路106は、そのまま、バケット・データ部の開始位置を検出するための状態となる。

【0200】そして、位置検出回路106は、バケット・データ部の開始位置を検出すると、データ保持回路108が保持しているPTSデータ、即ち、デスクランブルしようとするバケット・データ部と同一のバケットのバケット・ヘッダ部のPTSのデータ、あるいは、デスクランブルしようとするバケット・データ部と同一のバケットのバケット・ヘッダ部にPTSが存在しない場合には、PTSが存在するバケット・ヘッダ部のうち、直前のバケット・ヘッダ部のPTSデータを初期値として乱数発生器107に供給するように選択回路109を制御する。

【0201】ここに、EOR回路110においては、ディスク読み取り機構105から供給されるストリームのうち、デスクランブルの対象、即ち、スクランブルされているバケット・データ部のストリームと、乱数発生器107から出力される乱数とをEOR処理し、スクランブルされているバケット・データ部のストリームのデスクランブルが行われる。

【0202】また、位置検出回路106は、選択回路111を制御し、EOR回路110から出力されるデスクランブルされたストリームを出力し続けさせ、バケット・データ部のストリームが終了するまで待ち、その後、ディスク読み取り機構105から供給されるストリームをそのまま出力するようにさせる。

【0203】このようにして、ディスク読み取り機構105から供給されるストリームは、スクランブルされているバケット・データ部のストリームがデスクランブルされてなるストリームに変換され、MPEGデコーダ114に伝達される。

【0204】MPEGデコーダ114においては、PCMCIAカード98から供給されるストリームから映像データのストリームと音声データのストリームとが分離されて復号化され、映像データは、ディスプレイ115に伝達され、音声データは、スピーカ116に伝達される。

【0205】このように、本発明のデータ伝達方法及びシステムの実施の第4の形態においては、MPEG2-PS標準のストリームをスクランブルの対象とされているバケット・データ部のストリームをスクランブルして

なるストリームが格納されたディスク104から読み出されたストリームは、位置検出回路106及びPCMCIAカード98からなるデスクランブル回路によりデスクランブルされる。

【0206】ここに、位置検出回路106及びPCMCIAカード98からなるデスクランブル回路においては、スクランブルされているバケット・データ部のストリームごとに、デスクランブルしようとするバケット・データ部と同一のバケットのバケット・ヘッダ部にPTSが存在しない場合には、PTSが存在するバケット・ヘッダ部のうち、直前のバケット・ヘッダ部のPTSのデータ値を初期値として乱数発生器107に供給することにより、スクランブルされているバケット・データ部のストリームのデスクランブルが行われる。

【0207】このように、本発明のデータ伝達方法及びシステムの実施の第4の形態によれば、PCMCIAカード98の乱数発生器107には、スクランブルされているバケット・データ部のストリームごとに、データ値を一定としないPTSのデータ値が初期値として供給されると共に、CPU99から乱数発生器107に直接アクセスできないようにされているので、乱数発生器107から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【0208】なお、PCMCIAカード98に課金情報を持たせるようにすることができ、このようにする場合には、ディスク104から読み出される情報との課金が可能となる。

【0209】第5の形態・図11

図11は本発明のデータ伝達方法の実施の第5の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第5の形態）の要部を示すブロック図である。

【0210】図11中、117はカメラにより得られる映像データと、マイクにより得られる音声データとを符号化して時分割多重し、MPEG2-PS標準又はMPEG2-TS標準に基づくストリームにエンコードするMPEGエンコーダである。

【0211】また、118はMPEGエンコーダ117から出力されるストリームをスクランブルの対象とされているバケット・データ部のストリームがスクランブルされたストリームに変換するスクランブル回路である。

【0212】このスクランブル回路118は、本発明のスクランブル方法の実施の第4の形態の実施に使用するスクランブル装置であり、本発明のスクランブル装置の実施の第4の形態をなすものである。

【0213】スクランブル回路118において、119はMPEGエンコーダ117から出力されるストリーム

を格納するバッファメモリ、120はバッファメモリ119を制御するメモリコントローラ、121はバスである。

【0214】また、122は鍵信号により指定される系列の乱数を発生するDES規格の乱数発生器、123はMPEG2-PS標準のストリームについてのパケット開始コードの検出、PESスクランブル制御の内容の確認、PTS&DTSフラグの内容の確認、PTSの位置検出、パケット・データ部の開始位置検出及びMPEG2-TSのストリームについての同期バイトの検出、アダプテーションフラグの内容の確認、ペイロードフラグの内容の確認、PCRフラグの内容の確認、PCRの位置検出、ペイロード部の開始位置検出などを行う位置検出回路などとして機能するCPUである。

【0215】また、124はMPEGエンコーダ117から出力されるストリームがMPEG2-PS標準の場合とMPEG2-TS標準の場合とでCPU123の動作内容を変えるためのプログラムを格納するプログラムメモリである。

【0216】また、125は乱数発生器122に供給すべき初期値を格納する初期値レジスタであり、MPEGエンコーダ117から入力されるストリームがMPEG2-PS標準のストリームの場合にはPTSデータを格納し、MPEG2-TS標準のストリームの場合にはPCRデータを格納する。

【0217】また、126は初期値レジスタ125が保持するデータ値又は乱数発生器122から出力される乱数自身を乱数発生器122に供給する選択回路、127は選択回路126の選択動作を制御する選択制御レジスタである。

【0218】ここに、選択回路126は、CPU123がスクランブルの対象とされているパケット・データ部又はペイロード部の開始位置を検出すると、初期値レジスタが保持する初期値を乱数発生器122に供給し、その後、パケット・データ部又はペイロード部のストリームが終了するまで、乱数発生器122から出力される乱数をフィードバックするように選択制御レジスタ127の出力値により制御される。

【0219】また、128はバッファメモリ119から読み出されるストリームを格納するデータ・レジスタ、129はデータ・レジスタ128から出力されるパケット・データ部又はペイロード部のストリームと乱数発生器122から出力される乱数とをEOR処理し、スクランブルの対象とされているパケット・データ部又はペイロード部のストリームをスクランブルするEOR回路である。

【0220】また、130はデータ・レジスタ128から出力されるストリームと、EOR回路129から出力されるストリームとを選択して出力する選択回路であり、この選択回路130は、データ・レジスタ128か

ら出力されるストリームをスクランブルの対象とされているパケット・データ部又はペイロード部のストリームがスクランブルされてなるストリームに変換したストリームを出力するように制御される。

【0221】また、131は選択回路130から出力されるストリーム、即ち、スクランブル回路118から出力されるストリームを蓄積するディスク等の蓄積メディアである。

【0222】また、132は蓄積メディア131から供給されるストリームを、スクランブルされているパケット・データ部又はペイロード部のストリームがデスクランブルされてなるストリームに変換するデスクランブル回路である。

【0223】このデスクランブル回路132は、本発明のデスクランブル方法の実施の第5の形態の実施に使用するデスクランブル装置であり、本発明のデスクランブル装置の実施の第5の形態をなすものである。

【0224】このデスクランブル回路132において、133は蓄積メディア131から出力されるストリームを格納するバッファメモリ、134はバッファメモリ133を制御するメモリコントローラ、135はバスである。

【0225】また、136は乱数発生器122と同一の回路構成の乱数発生器であり、この乱数発生器136には乱数発生器122に使用された鍵信号と同一内容の鍵信号が供給される。

【0226】また、137はMPEG2-PS標準のストリームについてのパケット開始コードの検出、PESスクランブル制御の内容の確認、PTS&DTSフラグの内容の確認、PTSの位置検出、パケット・データ部の開始位置検出及びMPEG2-TS標準のストリームについての同期バイトの検出、アダプテーションフラグの内容の確認、ペイロードフラグの内容の確認、PCRフラグの内容の確認、PCRの位置検出、ペイロード部の開始位置検出などを行う位置検出回路などとして機能するCPUである。

【0227】また、138は蓄積メディア131から供給されるストリームがMPEG2-PS標準の場合とMPEG2-TS標準の場合とでCPU137の動作内容を変えるためのプログラムを格納するプログラムメモリである。

【0228】また、139は乱数発生器136に供給すべき初期値を格納する初期値レジスタであり、蓄積メディア131から供給されるストリームがMPEG2-PS標準のストリームの場合にはPTSデータを格納し、MPEG2-TS標準のストリームの場合にはPCRデータを格納する。

【0229】また、140は初期値レジスタ139が保持するデータ値又は乱数発生器136から出力される乱数自身を乱数発生器136に供給する選択回路、141

10

20

30

40

50

は選択回路 1 4 0 の選択動作を制御する選択制御レジスタである。

【0 2 3 0】ここに、選択回路 1 4 0 は、CPU 1 3 7 がスクランブルされているバケット・データ部又はベイロード部の開始位置を検出すると、初期値レジスタ 1 3 9 が保持する初期値を乱数発生器 1 3 6 に供給し、その後、バケット・データ部又はベイロード部のストリームが終了するまで、乱数発生器 1 3 6 から出力される乱数をフィードバックするように選択制御レジスタ 1 4 1 の出力値により制御される。

【0 2 3 1】また、1 4 2 はバッファメモリ 1 3 3 から読み出されるストリームを格納するデータ・レジスタ、1 4 3 はデータ・レジスタ 1 4 2 から出力されるバケット・データ部又はベイロード部のストリームと乱数発生器 1 3 6 から出力される乱数とを EOR 処理し、スクランブルされているバケット・データ部又はベイロード部のストリームをデスクランブルする EOR 回路である。

【0 2 3 2】また、1 4 4 はデータ・レジスタ 1 4 2 から出力されるストリームと、EOR 回路 1 4 3 から出力されるストリームとを選択して出力する選択回路であり、この選択回路 1 4 4 は、データ・レジスタ 1 4 2 から出力されるストリームをスクランブルされているバケット・データ部又はベイロード部のストリームがデスクランブルされてなるストリームに変換したストリームを出力するように制御される。

【0 2 3 3】また、1 4 5 はデスクランブル回路 1 3 2 から出力されるストリームから映像データのストリームと音声データのストリームとを分離して復号化する MPEG デコーダである。

【0 2 3 4】このデータ伝達システムにおいては、カメラにより得られる映像データとマイクにより得られる音声データとは、MPEG エンコーダ 1 1 7 によって、MPEG 2 - P S 標準又は MPEG 2 - T S 標準に基づくストリームにエンコードされ、スクランブル回路 1 1 8 に伝達される。

【0 2 3 5】そして、スクランブル回路 1 1 8 に供給されるストリームは、バッファメモリ 1 1 9 に格納され、バッファメモリ 1 1 9 に格納されたストリームは、CPU 1 2 3 により読み出される。

【0 2 3 6】ここに、MPEG エンコーダ 1 1 7 から出力されるストリームが MPEG 2 - P S 標準のストリームである場合には、CPU 1 2 3 は、バケット開始コードの検出、PES スクランブル制御の内容の確認、PTS & DTS の内容の確認、PTS の位置検出及びバケット・データ部の開始位置検出などを行う。

【0 2 3 7】そして、CPU 1 2 3 は、バケット開始コードを検出した場合、バケット・ヘッダ部のスクランブル制御の内容からバケット・データ部のストリームがスクランブルの対象とされているか否かを判断し、スクランブルの対象とされていない場合には、バケット開始コ

ードを検出するための状態に戻る。

【0 2 3 8】これに対して、バケット・データ部のストリームがスクランブルの対象とされている場合には、CPU 1 2 3 は、バケット・ヘッダ部の PTS & DTS フラグが “1 0” 又は “1 1” であるか否か、即ち、PTS の有無を判断する。

【0 2 3 9】判断の結果、PTS & DTS フラグが “1 0” 又は “1 1” の場合、即ち、PTS が存在する場合には、CPU 1 2 3 は、PTS の位置を検出して、PTS データを初期値レジスタ 1 2 5 に保持させ、バケット・データ部の開始位置を検出するための状態となる。

【0 2 4 0】これに対して、PTS & DTS フラグが “1 0” 又は “1 1” 以外の場合、即ち、PTS が存在しない場合には、CPU 1 2 3 は、そのまま、バケット・データ部の開始位置を検出するための状態となる。

【0 2 4 1】そして、CPU 1 2 3 は、バケット・データ部の開始位置を検出すると、初期値レジスタ 1 2 5 が保持する PTS データ、即ち、スクランブルしようとするバケット・データ部と同一のバケットのバケット・ヘッダ部の PTS のデータ、あるいは、スクランブルしようとするバケット・データ部と同一のバケットのバケット・ヘッダ部に PTS が存在しない場合には、PTS が存在するバケット・ヘッダ部のうち、直前のバケット・ヘッダ部の PTS データを初期値として乱数発生器 1 2 2 に供給するように選択制御レジスタ 1 2 7 の書換えを行う。

【0 2 4 2】ここに、EOR 回路 1 2 9 においては、データ・レジスタ 1 2 8 から出力されるストリームのうち、スクランブルの対象とされているバケット・データ部のストリームと、乱数発生器 1 2 2 から出力される乱数とが EOR 処理され、スクランブルの対象とされているバケット・データ部のストリームのスクランブルが行われる。

【0 2 4 3】この場合、CPU 1 2 3 は、選択回路 1 3 0 を制御し、EOR 回路 1 2 9 から出力されるスクランブルされたストリームを出力し続けさせ、バケット・データ部のストリームが終了するまで待ち、バケット開始コードを検出するための状態に戻る。

【0 2 4 4】このようにして、MPEG エンコーダ 1 1 7 から出力されるストリームは、スクランブルの対象とされているバケット・データ部のストリームがスクランブルされてなるストリームに変換されて蓄積メディア 1 3 1 に蓄積され、この蓄積メディア 1 3 1 に蓄積されたストリームは、適宜、デスクランブル回路 1 3 2 に供給されることになる。

【0 2 4 5】ここに、デスクランブル回路 1 3 2 に供給されるストリームは、バッファメモリ 1 3 3 に格納され、バッファメモリ 1 3 3 に格納されたストリームは、CPU 1 3 7 により読み出される。

【0 2 4 6】そして、CPU 1 3 7 は、バケット開始コ

10

20

30

40

50

ードを検出した場合、パケット・ヘッダ部のスクランブル制御の内容からパケット・データ部のストリームがスクランブルされているか否かを判断し、スクランブルされていない場合には、パケット開始コードを検出するための状態に戻る。

【0247】これに対して、パケット・データ部のストリームがスクランブルされている場合には、CPU137はパケット・ヘッダ部のPTS&DTSフラグが“10”又は“11”であるか否か、即ち、PTSの有無を判断する。

【0248】判断の結果、PTS&DTSフラグが“10”又は“11”の場合、即ち、PTSが存在する場合には、CPU137は、PTSの位置を検出して、PTSデータを初期値レジスタ139に保持させ、パケット・データ部の開始位置を検出するための状態となる。

【0249】これに対して、PTS&DTSフラグが“10”又は“11”以外の場合、即ち、PTSが存在しない場合には、CPU137は、そのまま、パケット・データ部の開始位置を検出するための状態となる。

【0250】そして、CPU137は、パケット・データ部の開始位置を検出すると、初期値レジスタ139が保持するPTSデータ、即ち、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部のPTSのデータ、あるいは、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部にPTSが存在しない場合には、PTSが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のPTSデータを初期値として乱数発生器136に供給するように選択制御レジスタ141の書換えを行う。

【0251】ここに、EOR回路143においては、データ・レジスタ142から出力されるストリームのうち、スクランブルされているパケット・データ部のストリームと、乱数発生器136から出力される乱数とがEOR処理され、スクランブルされているパケット・データ部のストリームのデスクランブルが行われる。

【0252】この場合、CPU137は、選択回路144を制御し、EOR回路143から出力されるデスクランブルされたストリームを出力し続けさせ、パケット・データ部のストリームが終了するまで待ち、パケット開始コードを検出するための状態に戻る。

【0253】このようにして、蓄積メディア131から出力されるストリームは、スクランブルの対象とされているパケット・データ部のストリームがスクランブルされてなるストリームに変換され、MPEGデコーダ145に伝達される。

【0254】他方、MPEGエンコーダ117からMP EG2-TS標準のストリームが出力される場合には、CPU123は同期バイトの検出を行い、パケット・ヘッダ部のスクランブル制御の内容からペイロード部のス

トリームがスクランブルの対象とされているか否かを判断し、スクランブルの対象とされていない場合には、同期バイトを検出するための状態に戻る。

【0255】これに対して、ペイロード部のストリームがスクランブルの対象とされている場合には、CPU123は、アダプテーションフラグからアダプテーション・フィールドがあるか否かを判断し、アダプテーション・フィールドがない場合には、CPU123は、ペイロードフラグからペイロードがあるか否かを判断する。

10 【0256】これに対して、アダプテーション・フィールドがある場合には、CPU123は、PCRフラグからPCRがあるか否かを判断し、PCRがない場合には、ペイロードフラグからペイロードがあるか否かを判断する。

【0257】これに対して、PCRがある場合には、CPU123は、PCRの位置を検出し、PCRデータを初期値レジスタ125に保持させ、ペイロードフラグからペイロードがあるか否かを判断する。

20 【0258】ここに、CPU123は、ペイロードがない場合には、同期バイトを検出するための状態となり、ペイロードがある場合には、ペイロード部の開始位置を検出するための状態となる。

【0259】そして、CPU123は、ペイロード部の開始位置を検出すると、初期値レジスタ125が保持するPCRデータ、即ち、スクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部のPCRのデータ、あるいは、スクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部にPCRが存在しない場合には、PCRが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のPCRデータを初期値として乱数発生器122に供給するように選択制御レジスタ127の書換えを行う。

30 【0260】ここに、EOR回路129においては、データ・レジスタ128から出力されるストリームのうち、スクランブルの対象とされているペイロード部のストリームと、乱数発生器122から出力される乱数とをEOR処理し、スクランブルの対象とされているペイロード部のストリームのスクランブルが行われる。

【0261】この場合、CPU123は、選択回路130を制御して、EOR回路129から出力されるスクランブルされたストリームを出力し続けさせ、ペイロード部のストリームが終了するまで待ち、同期バイトを検出するための状態に戻る。

50 【0262】このようにして、MPEGエンコーダ117から出力されるストリームは、スクランブルの対象とされているパケット・データ部のストリームがスクランブルされてなるストリームに変換されて蓄積メディア131に蓄積され、この蓄積メディア131に蓄積されたストリームは、適宜、デスクランブル回路132に供給されることになる。

【0263】ここに、デスクランブル回路132に供給されるストリームは、バッファメモリ133に格納され、バッファメモリ133に格納されたストリームは、CPU137により読み出される。

【0264】ここに、CPU137は、同期バイトの検出を行い、パケット・ヘッダ部のスクランブル制御の内容からペイロード部のストリームがスクランブルされているか否かを判断し、スクランブルされていない場合には、同期バイトを検出するための状態に戻る。

【0265】これに対して、ペイロード部のストリームがスクランブルされている場合には、CPU137は、アダプテーションフラグからアダプテーション・フィールドがあるか否かを判断し、アダプテーション・フィールドがない場合には、ペイロードフラグからペイロードがあるか否かを判断する。

【0266】これに対して、アダプテーション・フィールドがある場合には、CPU137は、PCRフラグからPCRがあるか否かを判断し、PCRがない場合には、ペイロードフラグからペイロードがあるか否かを判断する。

【0267】これに対して、PCRがある場合には、CPU137は、PCRの位置を検出し、PCRデータを初期値レジスタ139に保持させ、ペイロードフラグからペイロードがあるか否かを判断する。

【0268】ここに、CPU137は、ペイロードがない場合には、同期バイトを検出するための状態となり、ペイロードがある場合には、ペイロード部の開始位置を検出するための状態となる。

【0269】そして、CPU137は、ペイロード部の開始位置を検出すると、初期値レジスタ139が保持するPCRデータ、即ち、デスクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部のPCRのデータ、あるいは、デスクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部にPCRが存在しない場合には、PCRが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のPCRデータを初期値として乱数発生器136に供給するように選択制御レジスタ141の書換えを行う。

【0270】ここに、EOR回路143においては、データ・レジスタ142から出力されるストリームのうち、スクランブルされているペイロード部のストリームと、乱数発生器136から出力される乱数とをEOR処理し、スクランブルされているペイロード部のストリームのデスクランブルが行われる。

【0271】この場合、CPU137は、選択回路144を制御して、EOR回路143から出力されるデスクランブルされたストリームを出力し続けさせ、ペイロード部のストリームが終了するまで待ち、同期バイトを検出するための状態に戻る。

【0272】このようにして、蓄積メディア131から

出力されるストリームは、デスクランブル回路132において、スクランブルされているペイロード部のストリームがデスクランブルされてなるストリームに変換され、MPEGデコーダ145に伝達される。

【0273】このように、本発明のデータ伝達方法及びシステムの実施の第5の形態においては、MPEGエンコーダ117から出力されるMPEG2-PS標準又はMPEG2-TS標準のストリームは、スクランブル回路118において、パケット・データ部又はペイロード部のストリームをスクランブルしてなるストリームに変換され、蓄積メディア131を介して、デスクランブル回路132に供給され、デスクランブルが行われて、MPEGデコーダ145に伝達される。

【0274】ここに、スクランブル回路118においては、スクランブルの対象とされているパケット・データ部又はペイロード部のストリームごとに、スクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部のPTSのデータ、あるいは、スクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部にPTSが存在しない場合には、PTSが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のPTSデータ、又は、スクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部のPCRのデータ、あるいは、スクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部にPCRが存在しない場合には、PCRが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のPCRデータを初期値として乱数発生器122に供給することによって、スクランブルの対象とされているパケット・データ部又はペイロード部のストリームのスクランブルが行われる。

【0275】この結果、デスクランブル回路132においては、スクランブルされているパケット・データ部又はペイロード部のストリームごとに、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部のPTSのデータ、あるいは、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部にPTSが存在しない場合には、PTSが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のPTSデータ、又は、デスクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部のPCRのデータ、あるいは、デスクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部にPCRが存在しない場合には、PCRが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のPCRデータを初期値として乱数発生器122に供給することによって、デスクランブルの対象とされているパケット・データ部又はペイロード部のストリームのデスクランブルが行われる。

【0276】このように、本発明のデータ伝達方法及び

システムの実施の第 5 の形態によれば、デスクランブル回路 1 3 2 の乱数発生器 1 3 6 には、スクランブルされているバケット・データ部又はペイロード部のストリームごとに、データ値を一定としない P T S 又は P C R のデータ値が初期値として供給されることになるので、乱数発生器 1 3 6 から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができると共に、M P E G 2 - P S システム及び M P E G 2 - T S システムの 2 系列の伝送系に適用することができるので、利便性を高めることができる。

【 0 2 7 7 】

【発明の効果】以上のように、本発明のスクランブル方法を使用する場合には、デスクランブルは、スクランブルされている第 2 のストリーム部ごとに、第 1 のストリーム部内のデータ値が一定でない所定のデータを初期値として乱数発生器に供給することにより行われることになり、デスクランブル側の乱数発生器には、スクランブルされている第 2 のストリーム部ごとに、値を一定としない初期値が供給されることになるので、乱数発生器から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【 0 2 7 8 】また、本発明のスクランブル装置を使用する場合には、デスクランブル装置は、乱数を発生する乱数発生器と、スクランブルされている第 2 のストリーム部ごとに、第 1 のストリーム部内のデータ値が一定でない所定のデータを初期値として乱数発生器に供給する初期値供給回路と、スクランブルされている第 2 のストリーム部と乱数発生器から出力される乱数とを論理演算してスクランブルされている第 2 のストリーム部をデスクランブルする論理演算回路とを備えて構成されることになり、デスクランブル装置の乱数発生器には、スクランブルされている第 2 のストリーム部ごとに、値を一定としない初期値が供給されることになるので、乱数発生器から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【 0 2 7 9 】また、本発明のデスクランブル方法によれば、乱数発生器には、スクランブルされている第 2 のストリーム部ごとに、値を一定としない初期値が供給されることになるので、乱数発生器から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【 0 2 8 0 】また、本発明のデスクランブル装置によれば、乱数発生器には、スクランブルされている第 2 のストリーム部ごとに、必ずしも値を一定としない初期値が供給されることになるので、乱数発生器から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【 0 2 8 1 】また、本発明のデータ伝達方法によれば、本発明のスクランブル方法及び本発明のデスクランブル方法を使用しているのも、機密性の高いデータ伝達を

現することができる。

【 0 2 8 2 】また、本発明のデータ伝達装置によれば、本発明のスクランブル装置及び本発明のデスクランブル装置を使用しているので、機密性の高いデータ伝達を実現することができる。

【図面の簡単な説明】

【図 1】本発明のデータ伝達方法の実施の第 1 の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第 1 の形態）の要部を示すブロック図である。

【図 2】M P E G 2 - P S の P E S パケットの構造を示す図である。

【図 3】図 1 に示す本発明のデータ伝達システムの実施の第 1 の形態が備えるスクランブル回路の動作を説明するためのフローチャートである。

【図 4】図 1 に示す本発明のデータ伝達システムの実施の第 1 の形態が備えるデスクランブル回路の動作を説明するためのフローチャートである。

【図 5】本発明のデータ伝達方法の実施の第 2 の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第 2 の形態）の要部を示すブロック図である。

【図 6】M P E G 2 - T S のトランスポート・パケットの構造を示す図である。

【図 7】図 5 に示す本発明のデータ伝達システムの実施の第 2 の形態が備えるスクランブル回路の動作を説明するためのフローチャートである。

【図 8】図 5 に示す本発明のデータ伝達システムの実施の第 2 の形態が備えるデスクランブル回路の動作を説明するためのフローチャートである。

【図 9】本発明のデータ伝達方法の実施の第 3 の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第 3 の形態）の要部を示すブロック図である。

【図 1 0】本発明のデータ伝達方法の実施の第 4 の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第 4 の形態）の要部を示すブロック図である。

【図 1 1】本発明のデータ伝達方法の実施の第 5 の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第 5 の形態）の要部を示すブロック図である。

【図 1 2】従来のデータ伝達システムの一例の要部を示すブロック図である。

【図 1 3】図 1 2 に示すデータ伝達システムが有する問題点を説明するための図である。

【符号の説明】

2 2、4 3、6 9、1 1 7 M P E G エンコーダ

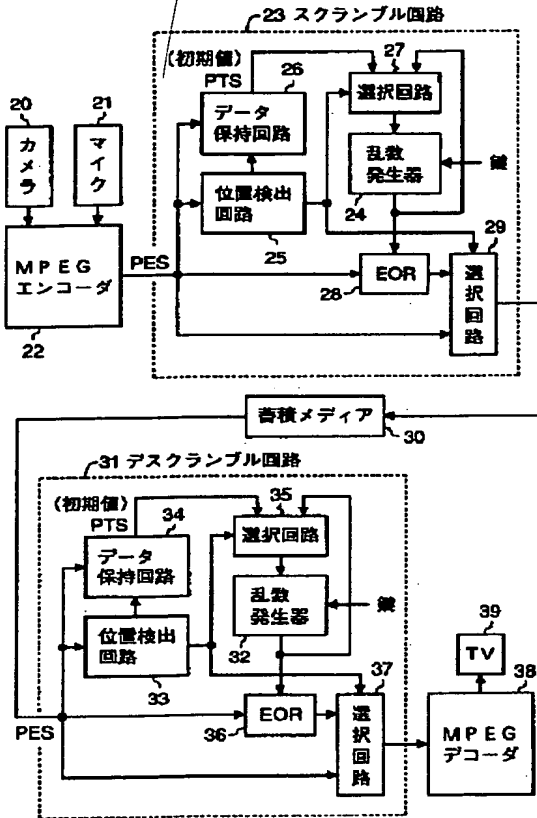
3 8、6 4、9 3、1 1 4、1 4 5 M P E G デコーダ

2 3、4 4、7 0、1 1 8 スクランブル回路

## 3 1、5 7、8 2、1 3 2 デスクランブル回路

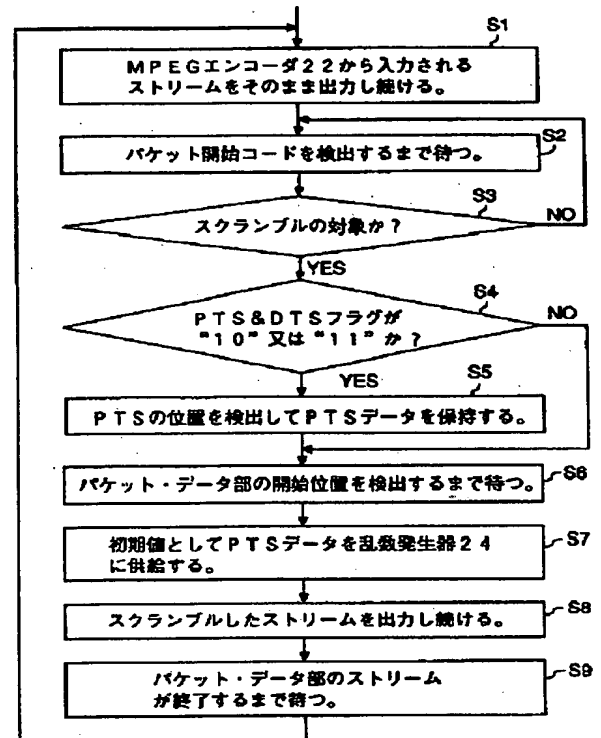
【図 1】

本発明のデータ伝達方法の実施の第 1 の形態の実施に使用するデータ伝達システム / (本発明のデータ伝達システムの実施の第 1 の形態) の要部を示すブロック図



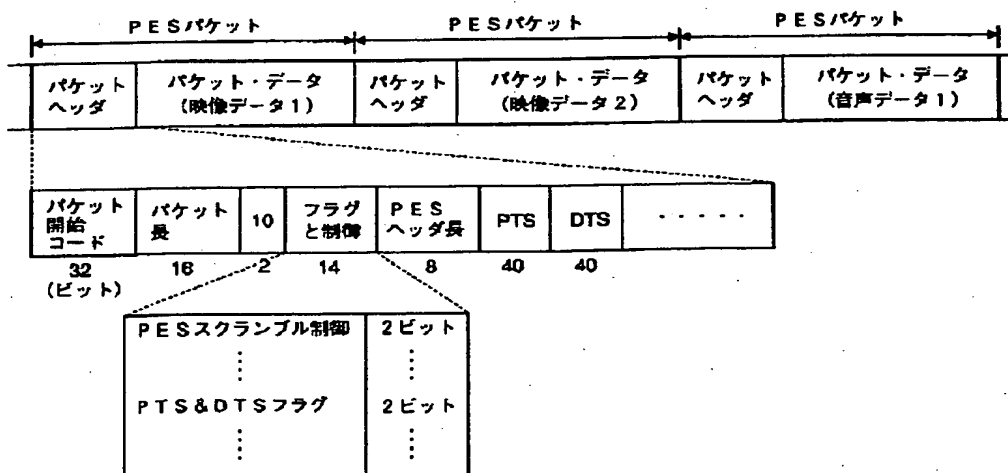
【図 3】

スクランブル回路 2 3 の動作 (本発明のスクランブル方法の実施の第 1 の形態) を説明するためのフローチャート



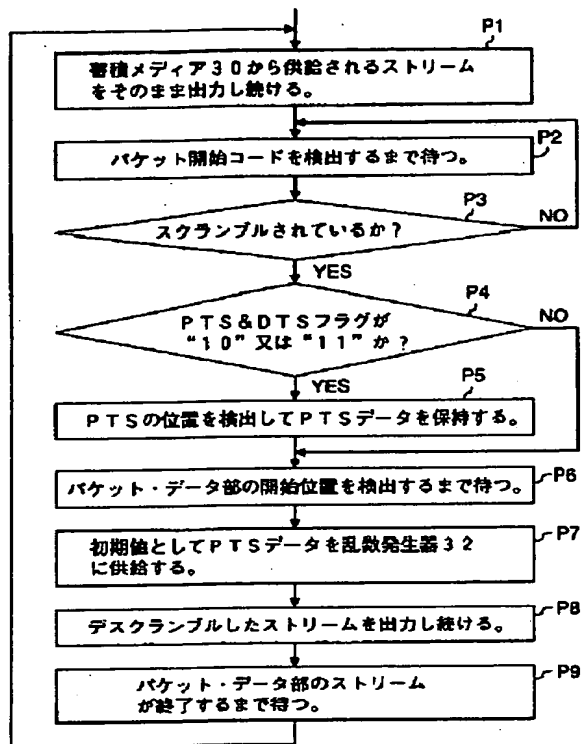
【図 2】

MPEG 2-PS の PES パケットの構造を示す図



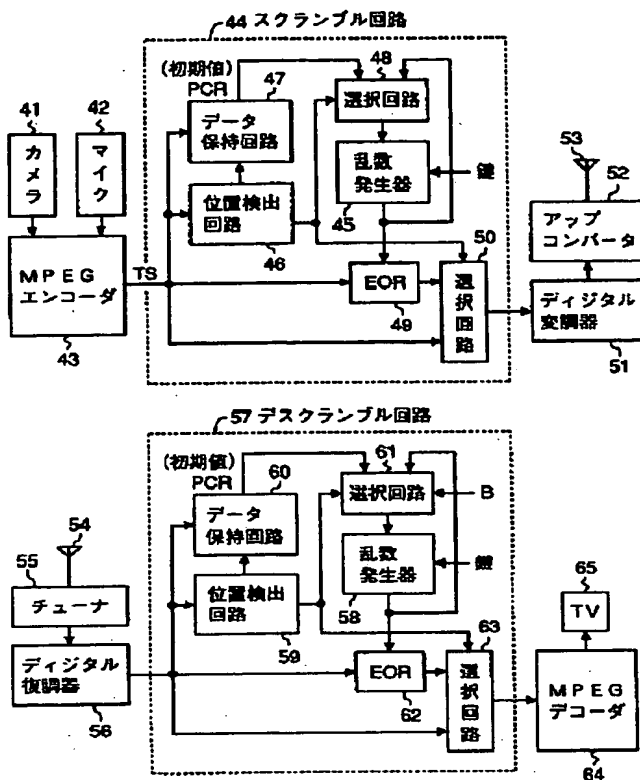
【図 4】

デスクランブル回路 31 の動作（本発明のデスクランブル方法の実施の第 1 の形態）を説明するためのフローチャート



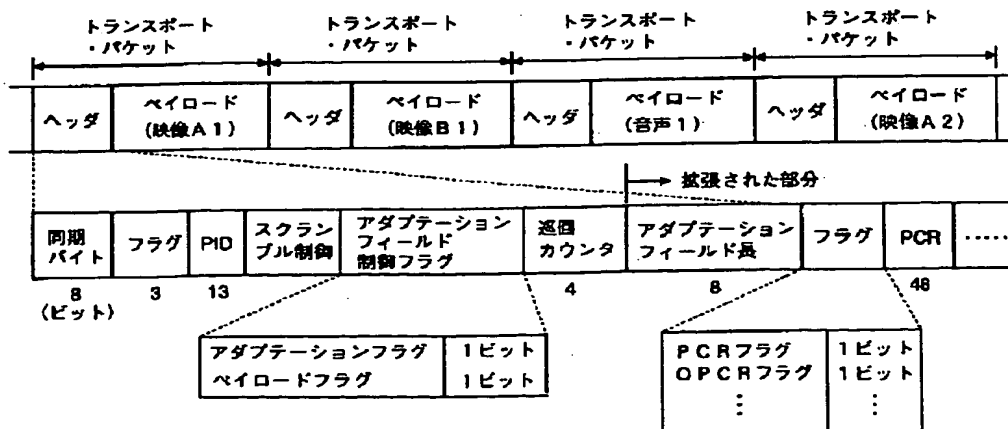
【図 5】

本発明のデータ伝達方法の実施の第 2 の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第 2 の形態）の要部を示すブロック図



【図 6】

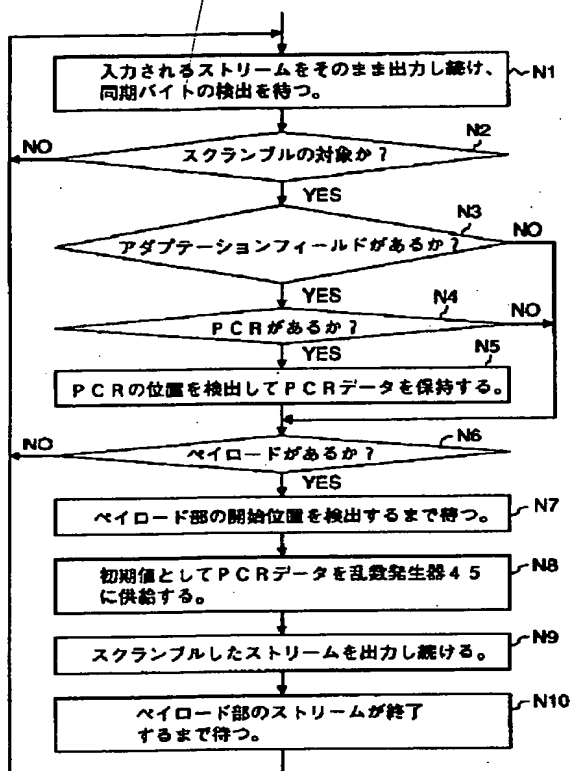
MPEG 2-TSのトランスポート・パケットの構造を示す図





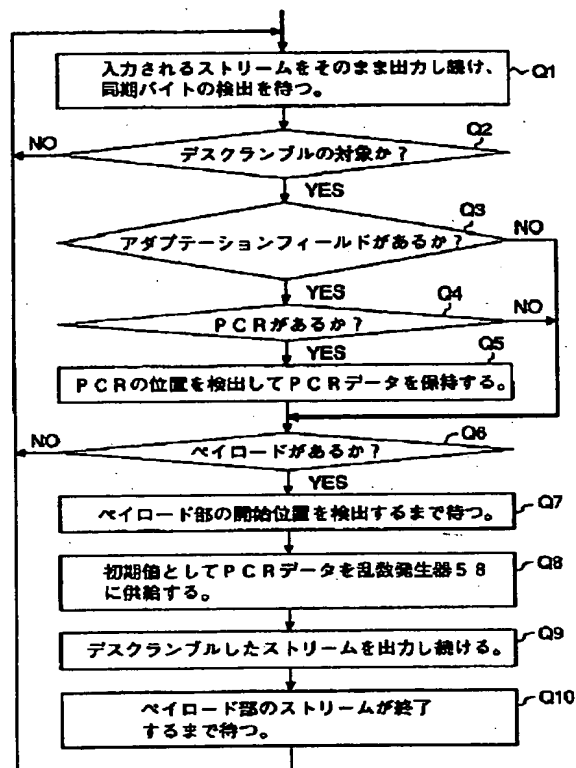
【图 7】

スクランブル回路 44 の動作（本発明のスクランブル方法の実施の第 2 の形態）を説明するためのフローチャート



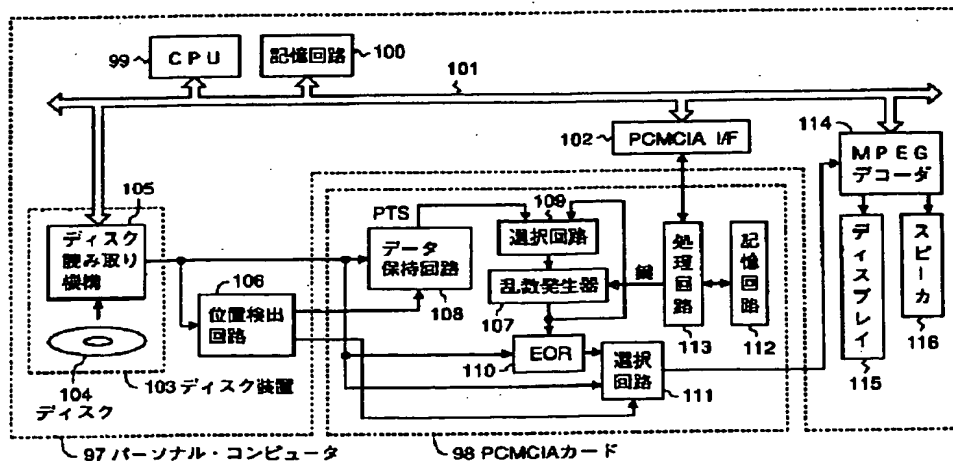
【图 8】

デスクランブル回路 57 の動作 (本発明のデスクランブル方法の第 2 の形態) を説明するためのフローチャート



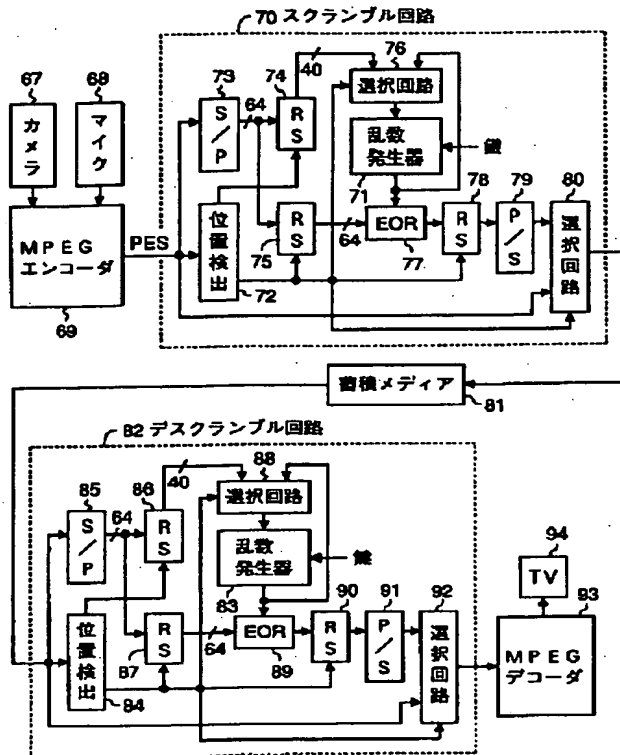
【図 1.0】

本発明のデータ伝達方法の実施の第4の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第4の形態）の要部を示すブロック図



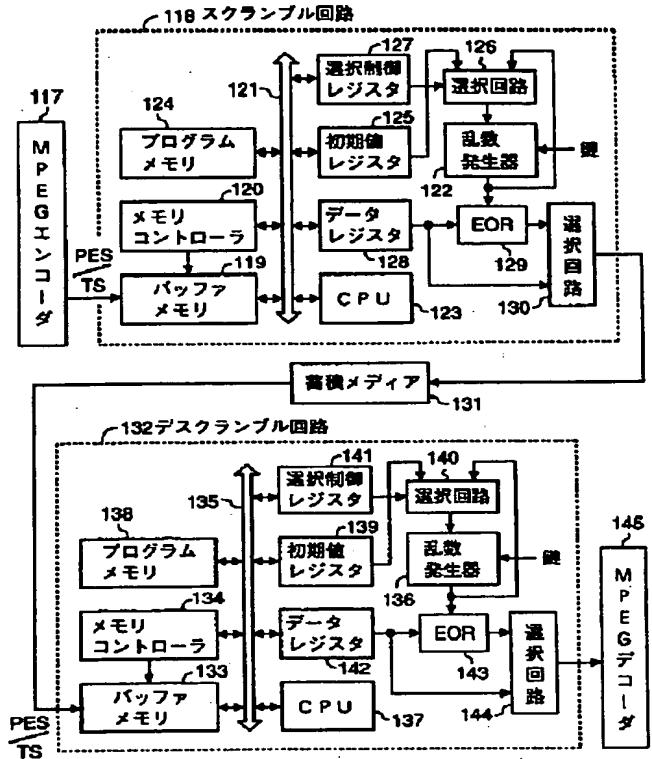
【図 9】

本発明のデータ伝達方法の実施の第 3 の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第 3 の形態）の要部を示すブロック図



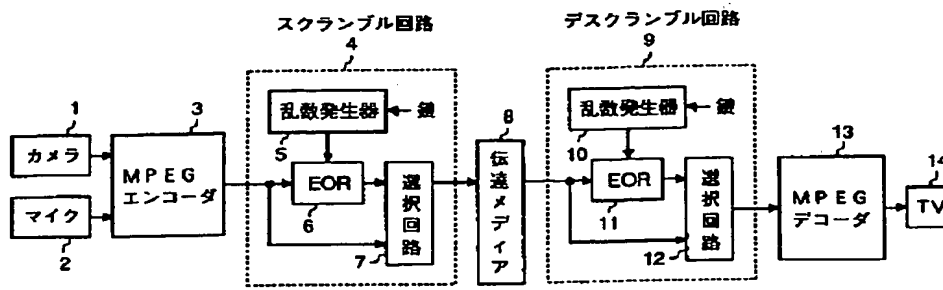
【図 11】

本発明のデータ伝達方法の実施の第 5 の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第 5 の形態）の要部を示すブロック図



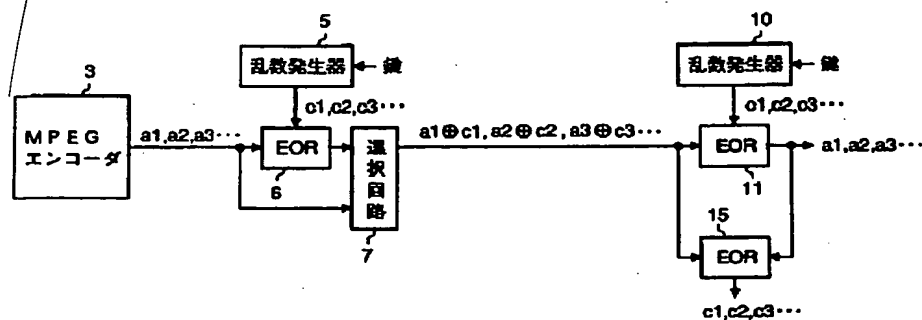
【図 12】

従来のデータ伝達システムの一例の要部を示すブロック図



【図 1 3】

図 1 2 に示す従来のデータ伝達システム  
が有する問題点を説明するための図



フロントページの続き

- (72) 発明者 秋山 良太  
神奈川県川崎市中原区上小田中 1 0 1 5 番  
地 富士通株式会社内
- (72) 発明者 飯島 清克  
神奈川県川崎市中原区上小田中 1 0 1 5 番  
地 富士通株式会社内